Draft Business Case *(DBC)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	

DRAFT BUSINESS CASE

Executive Summary

The Draft Business Case (DBC) document provides guidance on how to propose a business case for the development of a new, or modifications/enhancements to an existing, information technology (IT) investment. It establishes a formal agreement among the FAS' Management Council (MC) members on the high-level user's requirements, costs and schedule for an IT project. It also records management decisions to mitigate and accept a level of risk in the business, technological and project management environments.

The DBC is applicable to all MC-controlled IT projects. The responsibility for approving a DBC rests with the FAS' MC, CIO and Technology Review Board (TRB).

1.0 OVERVIEW

The DBC records the essential properties of the envisioned system in its early development stages and provides guidance on its achievement.

1.1 Purpose

Identify the system/project's purpose.

1.2 Background

DBC is meant to help the senior executives communicate between themselves and reach consensus on what they intend to achieve by pursuing this effort, and why. Provide information in this section on any previous decisions or system development projects that are relevant to understanding the current one.

2.0 MISSION

The strategic planning information here should refer to the FAS MC' strategic planning documents such as the Strategic and Performance Plans, IT Strategic Plan and the FAS' Enterprise Architecture (EA).

2.1 Value Statement

Convey why this system is necessary for your component. Relate the system value to the GSA and/or FAS mission.

2.2 Objectives

State the long-term component business objectives expected to be achieved by using the system.

2.3 Goals

State any quantifiable targets that your IT effort is to achieve, and the time frame for reaching them, as related to the proposed system. Goals must support one or more of the system objectives.

2.4 Critical Success Factors

Identify the factors that help the system to succeed in achieving the business goals provided above. They are defined as conditions which must exist *(or must be prevented)*. How will you know if this project is a success?

2.5 Performance Measures

For the above-mentioned business objectives, describe how the progress on their achievement will be measured and reported.

2.6 Enterprise Architecture Alignment

For the above-mentioned business objectives, describe how the business objectives align with the overall GSA Enterprise Architecture (EA). Current IT capabilities, planned IT programs, and ongoing projects, need to be understood in terms of how they relate to the GSA Business Architecture, Target Architecture, and high-level transition strategy. This identifies any existing solutions that may meet part of the business need that needs to be evaluated to facilitate leverage of existing capabilities and eliminates the development of duplicate functions within the GSA enterprise.

3.0 REQUIREMENTS STATEMENT

3.1 Existing Methods and Procedures

Provide a description of the current methods and procedures that will be employed to meet the existing requirements. Summarize the conclusions of any analysis that was performed on the existing system's ability to satisfy the mission, objectives, goals, and critical success factors described above. Describe the products and services delivered to the current customers.

3.2 Required Capabilities

3.2.1 Users' Requirements

Describe the user requirements in functional terms. This should be in narrative form and written from a users' perspective. Where helpful, graphical representations may be used to help the user express the requirements and their interrelationships. When a requirement is the improvement of existing methods and procedures, state extent of anticipated improvement and the relationship to the previously stated opportunities and deficiencies. Make sure that all of the functions included in the system are identified and that the functions are described in sufficient detail that an accurate estimate can be made of the resources required.

3.2.2 Data Sensitivity

Describe the requirements for protecting sensitive data. The sensitive information must be protected in accordance with the Federal Information Security Act of 2002 (*Public Law 107-347, Title III*).

3.2.3 Description

Define the life-cycle stages for all planned systems in this project:
□ New □ Upgrade □ Replacement

Who are the stakeholders for your project?
□ GSA □ Federal Agencies □ Public □ Other

Will the system integrate with other Agency systems?
□ Y □ N

Are you planning on using any resource intensive technologies?

Are you planning to make your application available from a GSA workstation?
□ Y □ N

What is highest sensitivity of data for your system(s)?
□ Confidential □ Public □ Secret

4.0 ASSUMPTIONS AND CONSTRAINTS

4.1 Organizational Structure

Identify the potential impacts on existing organizational structure. Identify scope change constraint to the current organization. Discuss the users, developers, maintainers and any other organizational units affected by the system. Define all constraints that the new organizational structure may impose on design and fielding of the system. Identify assumptions about who the users will be and where they will be physically located. Indicate any considerations for training, reassignment, etc.

4.2 Impact of Automation

What are the affects of automation on your current activities? Discuss decisions and assumptions that divide functions between people and machines. This establishes guidance on the functions that need manual intervention and automation's support of them. Reference the rationale for these decisions, such as cost benefit or other reasons *(union rules, re-training, computing limitations, etc.).*

4.3 Legal

Discuss legal considerations (pending legislation) that may affect the system development or use.

4.4 Security

Discuss any security considerations that may affect the system development or use.

4.5 Acceptable Alternatives

State any explicit flexibility in the application of technological approaches that system designers should consider. Adaptation and growth of the system should be discussed.

4.6 Organizational Support

Present the assumptions and constraints about the level of support to be provided by the organizations within and external to the project team that will participate in the development effort. All memorandums of understanding (MOU)s between these participants should be referenced here.

4.7 Budget

Identify assumptions and constraints affecting the project funds. For example, the effect variances from projected fee collections could have on the project in future fiscal years, the effect of proposed changes to the Federal budget or the assumption that the system can be developed within the approved budget.

4.8 Schedule

Identify externally imposed dates affecting the project. Also, identify assumptions and constraints about tasks or events on the critical path of the project schedule.

4.9 Other Projects

Identify dependencies between this project and other development or modification projects that relate to this project. Refer to any Memoranda of Understanding between the projects' Project Leads or System Development Managers.

5.0 ACQUISITION

Present any considerations for system procurement activities, including lead times and external and internal coordination.

5.1 Goals and Objectives

Detail the acquisition strategy objectives, e.g., developmental or non-developmental; risk reduction or transfer, timely deployment; reduction of the life cycle costs; standardize inventories; improve reliability; maximize use of current GSA infrastructure, logistics system, etc.

5.2 Constraints

Discuss any known constraints like the budget, schedule, operational, logistics, and maintenance or safety considerations. For IT systems, consider supportability, data sharing and interoperability requirements in the operational environment. The timing of the need for the planned capability will be addressed and an Initial Operational Capability (IOC) date will be stated.

5.3 Proposed Alternatives

Briefly discuss the range of acquisition alternatives to be considered.

6.0 PROJECT COST, SCHEDULE, AND PERFORMANCE

This section establishes the Sponsor and review board commitment to the schedule, funding and cost, and performance metrics for the project (i.e., the Investment Baseline).

6.1 SCHEDULE

Provide the major milestones and dates for the project. Specify the dates as a range if appropriate.

6.2 Approved Budget

State the requested budget for the life of the project by fiscal year. Indicate the funding sources which are providing funds to the project.

6.3 Project Life Cycle Cost Estimate (LCCE)

Present the estimated LCCE by fiscal year broken down into cost categories. The major cost categories are: personnel, hardware, software, security and supplies. The personnel costs shall show Government FTEs and contractors separately and be broken down into work breakdown structure (WBS) elements suitable for the investment.

6.4 Performance

State the measurable performance improvements anticipated from this project. Performance measures should be based on a stated period of time so that progress over time can be demonstrated. Examples can include system response times for the public/users, system availability, number of criminals denied access to guns due to data in the system, application processing times, etc.

6.5 Project Risks

Discuss potential risks and the reasonableness/acceptability of the costs of these risks, their probability, their costs, and mitigation strategies. Indicate if the cost figures have been adjusted to accommodate the risk calculations.

6.6 Return on Investment (ROI)

Discuss if quantitative and non-quantitative measures were used to indicate that the investment will provide a justifiable return relative to the investment level required. Indicate what quantitative and non-quantitative measures of valuation have been used to determine the ROI to the organization.

6.7 Affordability

Explain how the sponsoring organization will support this investment in light of other priorities.

Cost Benefit Analysis *(CBA)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

COST-BENEFIT ANALYSIS

Executive Summary

The Cost Benefit Analysis (CBA) effort analyzes and evaluates the candidate solutions to meet the stated need from a cost and benefit perspective. It also describes feasible alternatives, all tangible and intangible benefits and the analysis results. The feasible alternatives may be documented in more detail in a separate document, shown in Appendix C-4. This CBA will discuss which system costs are analyzed, present total costs for all the years the analysis covers, and outline the comparison between the costs of each alternative and the tangible benefits of the same.

Note: An urgent business need or external stakeholder pressure may dictate the use of an alternative development work pattern that may not identify, evaluate, or document alternative solutions. If no feasible alternatives are identified, the CBA methodology must be tailored to evaluate the costs and benefits of the proposed IT investment, without extensive analysis of alternative solutions.

1.0 OVERVIEW

Describes CBA's added value to the IT project and its justification as documented in OMB Circular A-11.

1.1 Purpose

This section discusses the CBA's intent on facilitating the GSA FAS' Go/No-Go decision about an IT investment project.

1.2 Scope

This section states the scope of the CBA.

1.3 Methodology

This section describes and discusses CBA's employed methodology and relationship to the SDLC work pattern to be used by the project team.

2.0 ASSUMPTIONS, CONSTRAINTS, AND CONDITIONS

The assumptions, constraints, and conditions form the foundation on which the CBA is based; a change in any one of these could cause a change in benefits as well as costs.

2.1 Assumptions

Assumptions are explicit statements used to describe the present and future environment on which an analysis is based. The assumptions relative to a project system may include:

- All data (that is, cost figures, workload statistics, benefit values, etc.) used in this analysis are assumed to be accurate, reliable, and valid;
- The results of this analysis could be skewed by inaccurate or different data;
- The expected useful life of the system is 5-7 years.

2.2 Constraints

Constraints are external factors that can limit the development of the application or the availability of the performance data from the current system. The constraints relative to a project may include:

- Any technology considered must be able to meet the minimum GSA business requirements;
- Otherwise, the programs and investments will be deemed cost ineffective and rejected by the FAS MC.

2.3 Conditions

Conditions are unique factors in the operating environment that may influence system processes. The conditions relative to a project may include:

- The technology used must allow integration into the existing or proposed environment;
- Redundant investment if more than one production platform is used;
- All alternatives must adhere to the principles of GSA Technical Reference Model (TRM);
- Alternatives implementing intranet or internet services will be in accordance with Agency policy.

3.0 FEASIBLE ALTERNATIVES

This section identifies the alternative solutions that can meet project's outlined needs and requirements. The results of the corresponding Feasibility Study are used as a starting point into an analysis of costs and benefits for the Feasible Alternatives identified in that study. Each Feasible Alternative is analyzed as documented in its own subsequent section (see Appendix C-4).

Here you can also describe the architecture on which the system will operate. This can be related to the local area network, wide area network, office automation, workstation security, and e-mail architecture already in place at the locations of deployment. The analysis must address conformance with TRM and all costs associated with upgrades or new development efforts. During the project development life, this section may need to be updated to include any changes or additions to the architecture.

Note: An urgent business need or external stakeholder pressure may dictate usage of iterative alternative development work patterns that may not identify, evaluate or document alternative solutions. If no Feasible Alternatives are identified, mark this section as Not Applicable.

3.1 Alternative 1

This section describes the alternative, its components and how it will work. Describe how the alternative meets the high-level functional requirements.

3.2 Alternative n

Repeat Section 3 for as many alternatives as available to the study. There must be, at the minimum, two alternatives present: Status Quo (on-going maintenance) and on-going maintenance plus enhancements. OMB, however, mandates four (including Status Quo) alternatives for all major IT investment.

4.0 COST ANALYSIS

This area presents the costs for design, development, installation, operation, maintenance and disposal and consumables for the development subject system. This profile is used to analyze the system costs for each year in its life cycle so those costs can be weighed against the benefits derived from its usage. According to OMB Circular A-94, the system is fully cost-accounted (including all spending resources,) whether appropriated or non-appropriated.

4.1 Cost Categories

Exhibit 4A, below, defines cost-related terms used in Cost Analysis (suggested line items may not be a complete list).

Terms and Definitions	Line Item
Nonrecurring Costs: Nonrecurring costs are developmental and capital investment costs incurred only once during analysis, design, development and implementation of the system.	• System development • Prototypes • Hardware purchase • Module design, development, and integration • System installation • Personnel
Recurring Costs: Recurring costs are incurred more than once throughout the life of the system and generally include operation and maintenance costs.	• Operations and Maintenance • Telecommunications • Supplies • Hardware and software upgrades, maintenance, and licenses • Personnel • Travel and training

Exhibit 4A. Cost-Related Terms.

4.2 Project Cost Analysis

The costs for system design, development, installation, operations and maintenance are presented in **Exhibit 4B**, below. This section explains that the costs for future years are discounted as per OMB A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs. The Year of real discount rate for number of years, and the Percentage Rate from OMB A-94, are used to derive the discount factors used in cost calculations. Discount factors are applied to the future years to provide an appropriate net present value (NPV) for system costs. Because of inflation, a dollar today is worth less in the future. It is important to recognize that dollar values of both benefits and costs associated with a project decrease over time because of inflation.

	Alternative 1	Alternative 2	Alternative 3
Year One			
Nonrecurring costs			
Recurring costs			
Year Two			
Nonrecurring costs			
Recurring costs			
Year Three			
Nonrecurring costs			
Recurring costs			
Total Costs			

Exhibit 4B. Cost Analysis.

A detailed description of cost breakdowns should be developed to explain exactly how cost calculations are presented. The discount rates should be applied where appropriate and documented as part of the explanation. Current acceptable rates to be used can be found in a current version of the OMB Circular A-94. If case of any scrutiny about the analysis, a line-by-line cost accounting should be presented.

5.0 BENEFIT ANALYSIS

This section analyzes the alternatives' individual ability to meet the goals of the project.

5.1 Key Benefit Terms

Exhibit 5A, below, lists and defines key terms used in this section.

Term	Definition
Tangible Benefits (paragraph 5.2)	• Benefits are expressed in dollars or in units. The result of tangible benefits may be: increased revenue, streamlined production, or saved time and money. For purposes of this analysis, tangible benefits are expressed in dollar values so that a valid comparison can be made with costs. • The benefits for future years are discounted as per OMB *A-94*, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs.
Intangible Benefits (paragraph 5.3)	• Benefits are expressed in terms of improved mission performance, • improved decision making, or more reliable or usable information. These • benefits may be quantifiable, but cannot be expressed in dollar values. • Many public goods are difficult to reliably and validly quantify in dollar • units; however, intangible benefits are vital to understanding the total • outcome of implementing a particular IT system.

Exhibit 5A. Key Benefit Terms.

5.2 Tangible Benefits

This section provides a detailed description of the tangible benefits. Because each alternative may not provide the same benefits, it is necessary to note which alternatives provide which benefits. The section also details the source(s) of data used to quantify benefit for each alternative and presents a chart that depicts its calculations. It is vital to provide sufficient documentation of data sources and calculations so that readers can follow the logic of the benefits quantification.

Exhibits 5A and 5B, below, detail this information. Repeat this for each tangible benefit.

Measurement		
Current Value	Alternative 1	Alternative n
Savings		

Exhibit 5A: Tangible Benefit 1.

Annual Transaction Times		
Current	Alternative 1	Alternative n
Savings		
FTE Savings		
FTE Savings	X FTEs	Y FTEs
Dollar Savings (Based on FTE Salary of $X per Annum)		
Dollar Savings		

Exhibit 5B. Annual Savings (Based on Average X Million Transactions per Annum).

Each benefit should be calculated for the number of projected years for each alternative. The benefits and costs for each alternative should be calculated for same number of years to provide an accurate cost benefit comparison. **Exhibits 5C and 5D**, summarize the quantifiable benefit value for each alternative and total tangible benefits for all alternatives, respectively

	Alternative 1	Alternative n
Benefit 1		
Benefit n		
Total Benefit		

Exhibit 5C. Tangible Benefits.

Tangible Benefit 1				
	FY03	FY04	FY05	Total
Alternative 1				
Alternative n				
Tangible Benefit *N*				
	FY03	FY04	FY05	Total
Alternative 1				
Alternative n				
Total Benefits				
	FY03	FY04	FY05	Total
Alternative 1				
Alternative n				

Exhibit 5D. Summary of Project Tangible Benefits. *Expected Return.*

5.3 Intangible Benefits

Even if no quantifiable dollar value has been placed on these benefits, they need to be related to value in some way if they influence the decision. Intangible benefits for each alternative may either be the same or different. It is important to include all intangible benefits.

Exhibit 5E shows expected return from the intangible benefits for three years, allowing for an accurate comparison with the three-year costs in Section 4.

Exhibit 5F illustrates a comparison of intangible benefits for each alternative, as well as, each technology solution as part of each alternative.

Intangible Benefits	Description
Intangible Benefit 1	
Intangible Benefit n	

Exhibit 5E. Intangible Benefits *Alternative 1*.

Intangible Benefits	Description
Intangible Benefit 1	
Intangible Benefit n	

Exhibit 5F. Intangible Benefits *Alternative N*.

For each alternative, include a table in the same format as the above exhibits.

Exhibit 5G, summarizes the values of intangible benefits for all alternatives.

Intangible Benefits	Alternative 1	Alternative n
Intangible Benefit 1		
Intangible Benefit n		

Exhibit 5G. Summary of Intangible Benefits. *Expected Return for All Alternatives.*

For comparison purposes, use Exhibit 5G to indicate if an alternative provides an intangible benefit, by placing a checkmark in the alternative box that does provide the particular benefit. It should be noted that if a tangible benefit can be valued in terms of units but not dollars, its valuation must be presented as an intangible benefit.

6.0 COMPARISON OF COSTS AND BENEFITS FOR PROJECT

This section compares a project's discounted costs and benefits. The first part of comparison examines the tangible benefits and the second part examines intangible benefits. The purpose of this comparison is to identify if tangible and intangible benefits outweigh the total cost of the system.

6.1 Comparison Results - Tangible Benefits

Exhibit 6A, below, compares the project's costs and Tangible Benefits (Identify what comparison tool was used.)

	Alternative 1	Alternative n
Total Tangible Benefits		
Total Costs		
Difference Between Costs and Benefits		

Exhibit 6A. Project Cost to Tangible Benefit Comparison.

6.2 Comparison Results - Intangible Benefits

Exhibit 6B, below, compares the Intangible Benefits of the project.

	Alternative 1	Alternative n
Intangible Benefits		

Exhibit 6B. Intangible Benefit Comparison.

Once you have determined the discounted values of costs and benefits, you need to compare each alternative. Methods that are commonly used to rank projects and compare alternatives are:

- Benefits/Cost Ratio (**BC**)
- Discounted Payback Period (**DPP**)
- Internal Rate of Return (**IRR**)
- Net Present Value (**NPV**)
- Return on Investment (**ROI**)

All of the above methods provide the expected analytical results for evaluation purposes equally well. Depending on their natures, however, different enterprises may opt for any, or a combination of all, of the above methods.

The FAS' preferred comparison method is BC which is defined as:

$$\mathrm{BC} = \frac{Total\_Benefits}{Total\_Implementation\_Costs}$$

It pertains to ratio between the net benefit of implementing an IT solution and its implementation cost. It depicts an organization's ability to profit (save costs) from an IT investment. The higher the ratio, the better an investment is.

APPENDIX A: REFERENCES AND DOCUMENTATION

Documents used to obtain information for this CBA, including project alternatives, costs, benefits, uncertainties, and information regarding cost-benefit methodologies, are listed in the subsequent sections.

APPENDIX B: GLOSSARY AND ACRONYMS

The definitions and acronyms presented in this section are specific to this analysis. Although these terms and acronyms may have other meanings, those included in the subsequent sections are used in this analysis.

Feasibility Study

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

FEASIBILITY STUDY

Executive Summary

Feasibility study is a preliminary study undertaken, before the full life-cycle work on a project begins, to ascertain the likelihood of a project's success. It is an analysis of possible solutions to a problem, upon completion of which, the resulting recommendations on the best solutions are presented in a clear, technology-independent fashion that is understandable, and agreeable to, by all affected organizations.

A project's feasibility is typically considered from *economic*, *organizationa*l, *schedule*, *technical* (and in some instances, *ecological*) viewpoints and contains decision criteria, comparisons of general solution possibilities and a proposed solution. Before conducting the study the following key questions must be addressed:

- What are the specific requirements, opportunities and the responsible organization(s)? Provide an initial recognition of requirement or opportunities and establish the broad objectives for the remainder of the life cycle. This decision addresses characteristics of the requirement or opportunity, such as programmatic or other causes and symptoms of the requirements or opportunities, affected organizations, types of information needed, high-level information processing capabilities, an initial perception of the ability of current systems and procedures to address the requirement or opportunity, and the timeframe(s) within which the requirement or opportunity must be resolved.
- What new information needs are associated with the problem? Devise a context for the future life-cycle decisions by determining if new information needs exist to support a solution. Define the scope of the needs in terms of missions and the affected organization(s).
- How broad a scope should the solution cover? Provide an overall context within which the potential solutions to the requirement are defined. Ensure that solutions focus on the major priority areas. The scope is determined in terms of the organization(s), such as agency offices, congressional organizations or executive branch agencies; pertinent portions of the missions or programmatic functions of each organization; and potential relationship of the current requirement and efforts to formulate its solution to other previously identified requirements and ongoing related efforts.

An inseparable companion to the feasibility study, cost benefit analysis (CBA) provides managers with adequate cost and benefit information to analyze and evaluate alternative approaches. CBA enables the top management to make decisions to initiate a proposed program or to [dis]continue the development, acquisition or modification of their information systems or resources.

1.0 OVERVIEW

1.1 Origin of Request

This section identifies the originator and describes circumstances that precipitated the request for this project request. Provide the objectives of the feasibility study in clear, measurable terms.

1.2 Explanation of Requirement

This section describes the requirements in programmatic technology-independent terms. It should state the specific deviation from the desired situation and the source and/or cause of the new requirement or opportunity. It also describes new information need(s), as well as cause(s) and effect(s) associated with the requirement or opportunity. Finally it validates the description of the requirement or opportunity with all affected organizations.

1.3 Organization Information

This section identifies organization(s) mentioned in Section 1.1, and their pertinent current procedures, information and systems. Provide descriptions of relevant procedures and systems as appropriate.

The section should specify all organizational units involved, list the organizational unit(s) at all levels of service, external organizations that relate to the requirement or opportunity and describe the pertinent mission area(s) and programmatic functions of each.

1.4 Glossary

Provide a glossary of terms and abbreviations used in the feasibility study.

2.0 EVALUATION CRITERIA

Identify the criteria applicable to evaluation of the study that was used to determine the recommended outcome. Such criteria typically include costs, functionality, ease of use, implementation considerations…

3.0 ALTERNATIVES DESCRIPTIONS

Describe every alternative proposed to handle the stated problem. Detail the resources required and its associated risk, system architecture, technology used and the manual process flow for each alternative. There must be, at the minimum, two alternatives presented: Status Quo (on-going maintenance) and on-going maintenance plus enhancements. OMB, however, mandates four (including Status Quo) alternatives for all major IT investment.

3.1 Alternative Model

For the proposed alternative, present a high-level data flow diagram and logical data model.

3.2 Description

Detail the required and desirable features and provide a concise narrative of the implementation effects of the proposed alternative.

4.0 ALTERNATIVE EVALUATION

Present the alternatives that were analyzed as part of the feasibility study along with the advantages and disadvantages appropriate for each alternative.

5.0 RECOMMENDATION

Present the recommended alternative. This should be the most advantageous alternative to implement and the optimum option to satisfy the previously stated needs.

Risk Management Plan *(RMP)*

(Version 2.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

mm/dd/yyyy

February 1st, 2012

Revision History

Version	Date	Summary of Changes
Version 1.0	02/2006	Initial Release
Version 2.0	02/2012	Updated to reflect emphasis on SEI CMMI and FAS OCIO Risk Management Process

RISK MANAGEMENT PLAN

EXECUTIVE SUMMARY

Risk management is the process of identifying, analyzing, and responding to project risks that could result in cost and schedule overruns, and project failure. Risk management begins with an assessment of the environmental, operational and technical risks prior to the establishment of a project.

Once the project has been approved and is initiated, risk management becomes an integral part of the project. Risk assessments should be conducted at logical checkpoints, or when key decisions are being made throughout the project. Risk assessment helps assure that positive events are maximized and that adverse events are minimized (i.e., that the response to the risk assures that the risk is avoided, mitigated, or accepted). The elements of risk management include identification, quantification, and response development and control.

Risk and Issue management must be applied throughout the entire project life cycle. Risk management is distinguished from "issue/problem management" in that risk management is concerned with situations that may or may not occur, whereas issue/problem management is concerned with known difficulties that are a result of a risk having occurred.

1 OVERVIEW

1.1 Purpose

Introduce the purpose of the Risk Management Plan. Include the name of the project, associated system(s), and the identity of the organization that is responsible for writing and maintaining this document.

This document describes the Risk Management Plan for the [identify Program/Project].

Risk Management is an ongoing activity performed throughout the life of the project to provide a control mechanism to monitor, report, and direct risk mitigation. Therefore, project risks will be updated on a timely basis and the status reported to the Project Manager, Division Director, and other key stakeholders as appropriate.

This document will be reviewed [annually] and updated as needed, as a result of continuous process improvement efforts by the project management team. Lessons learned will be captured at the end of each project phase. In addition to documenting the approach to risk identification and analysis, this plan identifies who is responsible for managing risks, how risks will be tracked throughout the project lifecycle, and how mitigation and contingency plans will be developed and implemented.

1.2 Scope

Present a definitive statement of the scope of the risk management planning, including the RMP's limits and constraints.

1.3 Policy

Provide policy decision statements that affect how the RMP is executed. List documents referenced to support the RMP. Also include any project or standards documents that are referenced in, or that have been used in the development of, the RMP document.

1.4 Definitions

The following definitions will be used relative to the Risk Management Plan:

- An ***issue*** is a situation or condition that either (1) currently has negative consequences or (2) has a 100% likelihood of having negative consequences within 30 calendar days
- A ***mitigating strategy*** is a proposed action that may be taken to offset the negative consequences of the risk in order to proactively manage potential risks
- A ***risk*** is a potential event that could have an unwanted impact on the cost, schedule, business, or technical performance. A risk becomes an issue when it occurs or is certain to occur
- ***Risk Management*** refers to the effort and process that is employed to reduce the negative impact that is caused by various risks
- ***Risk Matrix*** is a form used to capture and track all related information to a risk. It is currently an excel spreadsheet and can be found in Section 4 of this document

1.5 Approach

Provide a high level overview of the program/project's risk management process, for example:

1. Risk Identification: Identifying the risk as a true risk from data entered in the risk matrix (currently an excel spreadsheet).
2. **Risk Analysis:** Reviewing and ranking risks, and developing possible mitigation strategies or avoidance strategies for reducing the highest priority risks**;**

3. **Risk Response Planning:** Taking steps to contain or remove the risks identified during risk assessment and specifying the procedures needed to monitor the residual risks;
4. **Risk Implementation:** Monitoring the status of risks and the actions taken against risks to mitigate them;
5. **Risk Tracking and Control:** Applying the containment and monitoring techniques planned for the project, and reacting, reassessing, and reanalyzing as appropriate; and
6. **Risk Communications**: The status of existing risks and the assessment of new risks will be performed on a timely basis and reported to the appropriate stakeholders. Examples include the FAS OCIO Project Manager, FAS OCIO Division Director, QAPM, FAS OCIO Senior Management, and FAS/GSA governance boards as appropriate.

2 RISK MANAGEMENT PROCESS STEPS

2.1 Identify

> *Discuss the approach the project will use to identify risks. In general, risks are identified from working on similar projects (some of these can be gleaned from the Lesson Learned Reports) or through discussion with major stakeholders, end-users and customers. The following subsections describes the process used for many projects within FAS OCIO but should be tailored to reflect the program/project's requirements and environment.*

The risk identification process occurs throughout the project lifecycle. While the Project Manager has the primary responsibility for managing risk identification activities and collecting the identified risks for analysis, all project team members are responsible for identifying risks at a more granular level.

2.1.1 Conduct Risk Identification Reviews

The identification of risk is an individual responsibility as well as a team responsibility. Each member of the project team identifies risks associated with the project and documents them using a risk matrix.

The Risk Manager conducts a risk identification session with the project team and other stakeholders to identify potential programic risks. It can be beneficial to have a person serve as a recorder for this session to ensure all identified risks are captured.

The risk matrix is typically used to document all of the potential risks. During this session, only the Statement of Risk is completed on the risk matrix; follow-on steps in the risk management process will fill in other information.

An example list of common known risks in the software industry is:

- Budget, external constraints, politics and resources
- Capacity, documentation, familiarity, robustness, usability of methods, tools and supporting equipment that will be used in the system development
- Communication, cooperation, domain knowledge, experience, technical knowledge and training of the personnel associated with technical and support work on the project
- Complexity, difficulty, feasibility, novelty, verifiability and volatility of the system requirements
- Correctness, integrity, maintainability, performance, reliability, security, testability and usability of the SDLC work products
- Developmental model, formality, manageability, measurability, quality and traceability of the processes used to satisfy the customer requirements
- Internal and external threats to and vulnerabilities of the system and the information it stores, processes and transmits.

2.1.2 Document Risks

Define where the risk management tool is located and the process for updating the risk [identify the name and location of the Risk database].

When describing the risk, indicate the concern, likelihood, mitigating actions and possible consequences. Also describe the impacts to stakeholders, assumptions, constraints, relationship to other project risks, possible alternatives, as well as impacts to the project budget, schedule or deliverables.

Writing the Risk Statement: Identified risks are described and communicated to management in the form of risk statements. A risk statement provides the clarity and descriptive information required for a reasoned and defensible assessment of the risk's occurrence probability and areas of impact. A well-written risk statement contains two components. They are a statement of the Condition Present (e.g., If-then) and the Associated Risk Event (or events).

Example 1: Risk Statement

- *"If the team doesn’t get the required C++ training by November 1st, the project schedule will be slipped by 3 months.”*
- *Do not express risk statements in terms of a statement. For example, the previous risk statement should not be stated as “The project team requires C++ training by November 1st.”*

2.1.3 Validate Risks

Describe the process for validating the risks. Typically, the Project Manager is responsible for coordinating the review and validation of candidate risks with the Project Management team.

2.2 Analyze

Assign each risk to a Risk Owner for analysis. The Risk Owner analyzes it, determines what actions should be taken (if any), establishes the risk’s priority, and identifies the resources required to address the risk.

2.2.1 Categorize Risk

Group risks into categories by using the Risk Assessment Questionnaire. The Project Manager can create additional categories, as required. Assign the risk to a risk category. The risk category is assigned based on the type of anticipated impact.

2.2.2 Impact Analysis

Analysis is the conversion of risk data into risk decision-making information. It includes reviewing, prioritizing, and selecting the most critical risks to address.

The project team analyzes each identified risk in terms of its impact on cost, schedule, performance, and product quality. An individual risk may impact more than one of these categories. As shown by figure 2-1, risks are ranked as High, Medium, or Low for probability of the risk occurring.

Rank	Probability
High	Expected to occur (approximately >=70% likelihood)
Medium	Approximately 30-70% likelihood of occurring
Low	Not expected to occur, but still possible (approx. < 30% likelihood)

Figure 2-1.Risk Ranking Criteria

Second, the project team estimates the probability that each risk will occur and its time frame. As shown by figure 2-2, risks are ranked as High, Medium, or Low for the impact on the project should the risk occur.

Rank	Impact
High	Likely to cause maximum disruption to the project, resulting in the need to conduct re-

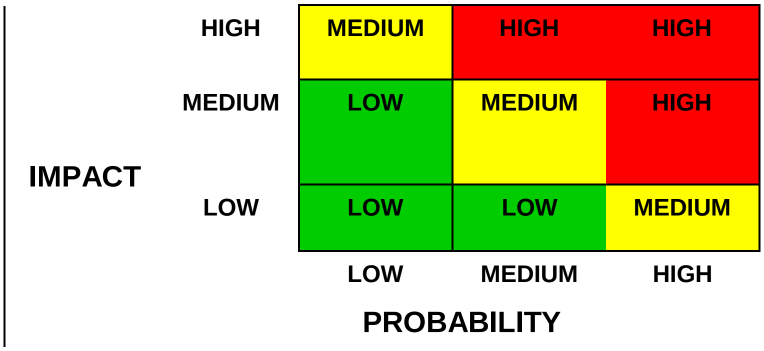
Rank	Impact
	planning and re-estimating.
Medium	Likely to cause significant delays or additional work that would exceed existing contingencies, resulting in exceeded time scales, additional resource and/or additional budget requirements.
Low	Likely to cause delays or additional work that could be contained within existing contingencies.

Figure 2-2.Risk Impact Criteria

The project team determines a risk level for each risk by mapping each risk onto a Risk Matrix, a sample of which is shown in figure 2-3. The project and risk management personnel evaluating the risk level for each risk can determine when appropriate mitigation action will be required. This decision making can be facilitated by the use of risk levels agreed to by the project team and project management where the risk levels are defined as:

- **L**ow Risk is a condition where risk is identified as having little or no effect or consequence on project objectives; the probability of occurrence is low enough to cause little or no concern.
- **M**edium Risk is a condition where risk is identified as one that could possibly affect project objectives, cost, or schedule. The probability of occurrence is high enough to require close control of all contributing factors.
- **H**igh Risk is the condition where risk is identified as having a high probability of occurrence and the consequence would have significant impact on project objectives, cost, schedule, and performance. The probability of occurrence is high enough to require close control of all contributing factors, the establishment of risk actions, and an acceptable fallback position.

At the conclusion of risk prioritization, a consolidated list of risks is created, and the updated risk matrix is placed under configuration management.



	HIGH	MEDIUM	HIGH	HIGH
	MEDIUM	LOW	MEDIUM	HIGH
IMPACT	LOW	LOW	LOW	MEDIUM
		LOW	MEDIUM	HIGH
		PROBABILITY		

Figure 2-3. Risk Impact and Probability Matrix

Consider the following areas for possible impacts.

- Cost / project budget
- Customer impacts

- HR resource requirements
- Organizational impacts
- Quality
- Security
- Schedule
- Scope / requirements
- Sponsor impacts
- User impacts

2.2.3 Review Risk Analysis and Ranking

The Project Manager presents the risk analysis for discussion at team meetings on a <weekly/biweekly/monthly> basis. At this meeting, discuss the impacts and possible mitigation/contingency options, and decide the risk's exposure (severity).

If the team decides risk actions are warranted, assign a Risk Owner and task them with creating the appropriate mitigation and/or contingency action plans. Discuss the risk that may be considered sensitive or confidential and, if appropriate, consult with Legal.

Review the newly identified risk. Establish its relative rank among existing risks and review the risk in combination with other risks (for example, risks in a similar functional area or with similar impacts). Adjust resource assignments, action plans, or other project priorities to ensure the risk is adequately addressed.

2.2.4 Update Risk Log

After review, the Project Manager will update the Risk Log with any comments and document the next steps for the risk (if any). If the ranking of the risks has changed in the Risk Log, the Project Manager updates the ranking to reflect current priorities and concerns.

2.3 Plan

Risk planning involves developing plans for mitigation and/or contingency actions for a specific risk.

- Identify mitigation and contingency actions for funding, schedule, staff or resources.
- Assign actions as appropriate and ensure these fit within the project's budget and schedule.
- Determine the actions to reduce the likelihood or consequences that impact on the project.
- Determine the response based on a cost/benefit analysis (cost vs. benefit).
- Describe the actions to mitigate the risk.
- Describe the signs that may be indicators of Risk Event occurrence.
- Describe the contingency plan for when the risk event occurs.
- Assign responsibilities for each response with a "due date".
- Determine impact on project budget and schedule. Update the project plan where necessary.
- Update the Risk Log with this information.

2.3.1 Plan Mitigation Activities

Capture the following information in the risk mitigation plan(s).

- Desired outcome of the mitigation activities.
- How and when mitigation activities will be tracked?
- Mitigation strategies to be implemented.
- Which Risks are to be mitigated?

- When each mitigation activity will commence / cease?
- Who is responsible for the mitigation activities?
- Who is responsible for tracking mitigation effectiveness and how is effectiveness measured?

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these major categories

1. *<u>Risk Acceptance</u>*

   This approach is employed because the risk items are the result of external factors over which you have no control. There is also no effort made to avoid risk. Two actions are usually taken under this approach:

   - Contingency Planning. Where you plan contingencies in case the risk does occur. Thus, the project team has a backup plan to minimize the risk affects.
   - No Action. Where you take no action and accept the responsibility for the risk.

2. *<u>Risk Avoidance</u>*

   This approach is the act of not performing an activity that could carry a risk. An example would be not buying a property or business to not take on the liability that comes with it. Another would be not flying to not take the risk that the airplane would crash.

   Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting it may have allowed. Not entering a business to avoid the risk of loss also prevents one from the possibility of earning profits.

3. *<u>Risk Mitigation</u>*

   This method emphasizes reducing the severity of a loss by avoiding, preventing or reducing a risk. Reducing the number of requirements or defining them more completely can avoid some risks.

   For example, careful definition of the project scope in the SOW can help avoid possible consequence of "scope creep," or indecisive, protracted and uncertain scope objectives.

4. *<u>Risk Transfer</u>*

   This method means causing another party to accept the risk, typically by contract or hedging. With the transfer approach, the objective is to reduce risk by transferring it to another entity that can better bear it.

Review the risk items with high rankings and determine if the significant risks will be accepted, avoided, mitigated or transferred.

2.3.2 Plan Contingency Activities

Develop a contingency plan for those risks where it is unlikely or uncertain that the mitigation will be effective. Capture the following in the risk contingency plan.

- Description of the risk.
- Anticipated effects on project budget and schedule.
- Anticipated effects on staff, users, and stakeholders.
- Anticipated effects on work products or deliverables.
- Desired outcome of contingency activities.

- How to evaluate and track the contingency activities
- What activities will be executed to minimize the risk's effects
- When will the activities occur (i.e. trigger event)?
- When will the contingency activities cease?
- Who is responsible for the activities?

2.3.3 Review Risk Action Plans

Identify who reviews the risk action plans and presents them at the <meeting/frequency>. In general, this will be the Risk Owner and Project Manager.

The project team reviews the plans, trigger events, resources required, and measurements for tracking effectiveness. This will ensure they are feasible and appropriate for the severity and ranking of the risk. The team may propose additional actions or changes, as appropriate, and may request to review the updated plans before their implementation.

2.3.4 Update Risk Log

Identify who is responsible (i.e. Risk Owner) for documenting the plans and forwarding them to the Project Manager for inclusion in the Risk Log. The Project Manager reviews the status of action planning activities <biweekly/monthly> in the <meeting

2.4 Track

Risk Plan implementation involves executing the decisions made in the Risk Mitigation and/or the Risk Contingency plans. Mitigation and contingency plans are a) tied to a trigger event and executed when that event occurs, or b) implemented immediately.

2.4.1 Monitoring Trigger Events

The Risk Owner is responsible for monitoring the trigger events associated with mitigation/contingency actions. The Project Manager assists with tracking triggers as part of the risk status review meeting.

2.4.2 Executing Action Plan

The Risk Owner executes the action plan as follows:

- Initiates the mitigation/contingency plan and notifies the Project Manager of the plan execution when the trigger event occurs or is imminent.
- Notifies all parties identified in the mitigation/contingency plan and ensures all activities are coordinated.
- Takes specific measurements to determine the effectiveness of the activities
- Notifies the Project Manager if the activities are not producing the desired effect and proposes changes to address the deficiencies.

2.4.3 Updating The Risk Log

The Risk Owner provides status updates to the Project Manager who then updates the Risk Log to reflect the actions being taken (i.e. date of trigger event etc.).

Action plan activities and their effectiveness are monitored in the <weekly/biweekly/monthly> <status review meeting>.

2.5 Risk Tracking, Monitoring & Control

The Risk Tracking, Monitoring and Control concerns how the risk is progressing, as well as any mitigation/contingency strategies that have been executed. When changes to the risk occur, repeat the cycle of identify, analyze, and plan. Modify existing action plans to change the approach if the desired effect is not being achieved.

Factors to consider for Risk Tracking include:

- Assess all risks as defined in the Risk Log
- Ensure all requirements of the Risk Management Plan are being implemented
- Establish communications
- Evaluate the effectiveness of actions plan taken
- Highlight new assumptions
- Identify new risks
- Identify the status of actions to be taken
- Track risk response
- Validate previous assumptions
- Validate previous risk assessment

Factors to consider for Risk Control include:

- Validate mitigation strategies and alternatives
- Take corrective action when events occur
- Assess impact on the project of actions taken (i.e. cost, time, resources etc)
- Identify new risks resulting from mitigation actions
- Ensure the Project Plan is maintained
- Ensure change control addresses risks associated with the proposed change
- Revise the Risk Assessment Questionnaire, Risk Assessment Checklist and other risk management documents to capture results of mitigation actions.
- Revise the Risk Log

2.6 Communicate

Discuss the approach to communications throughout the project's life cycle. Communications regarding risks must be continuous throughout the life-cycle, both through verbal and written reports.

2.6.1 Status Meetings

Discuss risk management activities at status meetings and include identification and status of individual risk activities and assignments. Capture the risks' status in the meeting minutes and circulate as appropriate.

On a <weekly/monthly> basis, the Risk Owners sends updates to the Project Manager who then updates the Risk Log. All open risks and action plans are reviewed with the project management team as well as the results and effectiveness of mitigation/contingency actions and the status of trigger events and risk profiles.

2.6.2 Lessons Learned

The Project Manager documents the result of risk actions (i.e. successful/unsuccessful) and lessons learned in the Risk Log. At the end of each phase, the Project Manager discusses the lessons learned with the [functional leads], as appropriate.

When a project closes, the Project Manager leads a Final Risk Review to document the final status, results of mitigation and contingency actions, and to identify lessons learned during the project. These lessons learned on risk management are shared with other projects and used to update the Organization's policies, standards and templates, as appropriate.

2.6.3 Escalate Risks

Define the process and threshold for escalating the risk. Typically, the Project Manager is responsible for performing risk reporting and escalating risks. The Project Manager will discuss the status of the risk with the [FAS CIO PMO representative] and the Project Sponsor. The project then escalates the risk to the [Project Stakeholders] and forwards a copy to [Key Stakeholder] as appropriate.

2.6.4 Retiring Risks

Close risks when the risk event actually occurs or when the likelihood of the risk is reduced such that it is not worth tracking it. At this time, halt and close action plans. If the risk could possibly arise again, reduce the risk to a “Watch” status and evaluate periodically.

The Project Manager makes the final decision to retire a risk. In some cases, the Project Sponsor may be involved in the decision to retire a risk.

2.7 Issue Management

Issue management is undertaken during the ‘Execution’ phase of the project (i.e. the phase within which deliverables are produced), Project issues may be identified at any stage of the project lifecycle. In theory, any issue identified during the life of the project will need to be formally managed as part of the Issue Management Process. Without a formal Issue Management Process in place, the objective of delivering a solution within ‘time, cost and quality’ may be compromised.

Issue Management Process Diagram

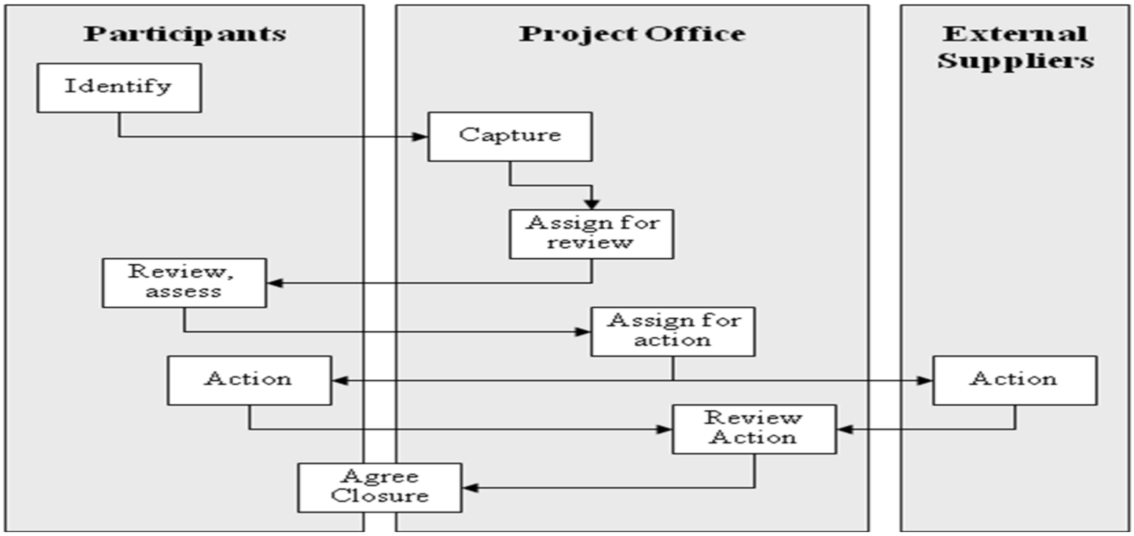


Figure 2-4. Risk Issue Management Process Diagram

2.7.1 Issue Log

The most important control tool is a log summarizing the issues, their current status and who is currently responsible for them; this can be accomplished using technical forms or a fully integrated database.

2.7.2 Issue Management at Phase End

Although the project team will be striving to resolve issues in the most beneficial way, some may remain unresolved at the end of a phase. The Project Manager will need to review the status of the outstanding issues and consider what impact they may have. The phase-end reporting should include any significant outstanding issues and will summarize the overall impact on the benefit model. Any consequences should be agreed with the Project Sponsor and Steering Committee.

Outstanding issues will form an input into the detailed planning process for the following phase of work.

2.7.3 Completing the Issue Management Process

The Project Manager and teaming will be reviewing the outstanding issues on a regular basis and proactively tracking them to conclusion. By the end of the project there should be no outstanding issue left to resolve. This does not mean that every issue can be dealt with during the project. It may be that some concerns cannot be dealt with and appropriate responses should be made to those concerned. Other issues may be deferred to be addressed either as part of the live maintenance of the system or in a future project.

The final status of the issues should normally be reported and reviewed with the Project Sponsor and project leadership as part of the finalization of project. Specific actions or requests for future work would be passed into the relevant management processes and potentially tracked as part of lessons learned.

3 ROLES & RESPONSIBILITY

Provide a list of the specific groups or individuals involved in the project's risk and issue management activities, and then describe their respective tasks and responsibilities. In some cases, the same individual may perform multiple roles across the organization.

The Project Manager is responsible to train all project staff on their responsibilities when they join the project.

3.1 Project Team

Describe the roles and responsibilities of the Project Management Office (PMO), i.e. those individuals providing support to the Project Manager.

The PMO representative(s) defines and maintains project management standards across the organization. It is also the source of documentation, guidance and metrics on the practice of project management and execution.

Role	Responsibility / Task
Government Project Manager	▪ Approves the Risk Management Plan. Participates in risk mitigation, contingency planning, execution, and decisions on risk actions. ▪ Responsible for leading the risk management effort, sponsoring risk identification activities, facilitating communication, ensuring the Risk Log is maintained, and that risk activities are current. ▪ Responsible for ensuring risks are being managed in accordance with the Risk Management Policy and the Risk Management Plan. The Project Manager also assists in identifying new risks and/or proposing mitigation strategies and contingency plans, and proposing process improvements to the risk management plan and processes.
Contractor Project Manager	▪ Participates in risk mitigation, contingency planning, execution, and decisions on risk actions. ▪ Responsible for sponsoring risk identification activities, facilitating communication, ensuring the Risk Log is maintained, and that risk activities are current. ▪ Responsible for ensuring risks are being managed in accordance with the Risk Management Policy and the Risk Management Plan. The Project Manager also assists in identifying new risks and/or proposing mitigation strategies and contingency plans, and proposing process improvements to the risk management plan and processes.
Project Team	▪ Participates in the risk identification process, and discusses risk monitoring and mitigation activities at team meetings. Participants will include team members, consultants and contractors.
Risk Owner	▪ Responsible for managing an individual risk.
Directors	▪ Responsible for ensuring risk analysis is completed, risk mitigation/contingency strategies are developed, and plans are executed successfully.
PMO	▪ Responsible for providing FAS CIO PMO policy, guidance, templates and documentation to support project lifecycle. ▪ Responsible for monitoring risk identification activities, facilitating communication, ensuring the Risk Log is maintained, and that risk activities are current.

3.2 Project Sponsor

The Project Sponsor provides the interface between project ownership and delivery. They act as a single point of contact with the Project Manager for the day-to-day management of the interests of the client organization. This person must have adequate knowledge about the business and the project to make informed decisions. They are may sometimes referred to as the Project Director.

Role	Responsibility
Project Sponsor	▪ Participates in risk identification and risk activities as part of the project team. The Sponsor executives also receive escalated risks and assist with mitigation and contingency actions for escalated risks, as needed. The Project Sponsor for this project is [Identify Project Sponsor].

3.3 Other Participants

Role	Responsibility
Project Stakeholders	▪ Identify the project stakeholders, for example, Steering Council, Executive Board etc. The stakeholders' role is to monitor risk action effectiveness and participate in risk escalation.
Legal	▪ Provides advice on risks which may have legal ramifications and/or which are of a sensitive nature.
Security	▪ Security Team provides an Independent Verification and Validation oversight of the project and report to external stakeholders. The Security Team may perform their own risk identification interviews/reviews, may participate in project risk meetings and reviews, and may request risk reports and status from the Project Manager.

4 TOOLS, TECHNIQUES & REPORTS

Identify the tools and techniques that will be used to store risk information, evaluate risks, track the status of risks or generate risk management reports.

4.1 Risk Management Software

Identify the software used for managing risk management activities.

[Identify Software] is a risk management database designed to describe, organize, prioritize, track and display project risks. The application provides standard database functions to add and delete risks, specialized functions for prioritizing and retiring project risks, as well as maintaining a log of historical events.

Contact the FAS CIO PMO Team if you require an alternate method for Risk Management Reporting.

Software	Purpose	Owner
Risk Log	Identify its purpose	Identify Owner
Issue Log	Identify its purpose	Identify Owner

4.2 Risk Management Reports & Reviews

The following reports are delivered in support of the Risk Management Plan:

Report Name	Purpose	Frequency	Audience
Report Name	Describe its purpose	Weekly / Biweekly / Monthly	Project Team, Project Board, Client
Report Name	Describe its purpose	Weekly / Biweekly / Monthly	Project Team, Project Board, Client
Report Name	Describe its purpose	Weekly / Biweekly / Monthly	Project Team, Project Board, Client
Report Name	Describe its purpose	Weekly / Biweekly / Monthly	Project Team, Project Board, Client

The following table defines the minimal list of required fields as part of the risk log.

<table>
<tr><th colspan="10">Risk Log</th></tr>
<tr><td colspan="10"><i>Project Name:</i></td></tr>
<tr><th>Risk Name</th><th>Description</th><th>Probability</th><th>Impact</th><th>Priority</th><th>Mitigation Strategy</th><th>Contingency Plan</th><th>Owner</th><th>Due Date</th><th>Status</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Figure 2-5. Risk Log Template

5 ACRONYMS

Term	Meaning
CDR	Critical Design Review
DR	Decision Review
IV&V	Independent Verification and Validation
LCC	Life-Cycle Cost
MIS	Management Information System
MS	Milestone
O & M	Operations and Maintenance
PM	Project Manager
PMO	Program Management Office
PSR	Program Status Report
RMP	Risk Management Plan
RTR	Risk Tracking Report
SOW	Statement of Work
WBS	Work Breakdown Structure

Configuration Management Plan *(CMP)*

[Template]

(Version 2.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

mm/dd/yyyy

March 1st, 2012

TABLE OF CONTENTS

REVISION HISTORY

Version Number	*Description*	*Date*
Version 1.0	*Initial Release*	
Version 2.0	*Updated template*	

EXECUTIVE SUMMARY

[*Italicized text is guidance and reference only and should be deleted prior to completing the document.*

All sections identified in the Table of Contents must remain in the document. Additional subsections may be added as required]

Configuration Management (CM) is a uniform practice for managing changes in software, hardware and documentation throughout the acquisition or development project.

The CM plan should be produced as part of the project planning phase of the SDLC.. The CM activities should continue throughout the life of the delivered end-product, and therefore, at the project's end, the adopted approach should be transferable to the organization responsible for operational maintenance. The executive summary should be an overview of the CM plan, highlighting the major points of each section in the plan.

1 OVERVIEW

Provide a statement that introduces the CM plan and describes, in general terms, its use in managing the configuration of the specific project, or system. Also, briefly discuss the roles and responsibilities of key participants and how CM will be applied. Below are representative paragraphs that can supplement the overview statement(s):

CM Concepts *– CM is an integral part of acquisition, development and program management for all that constitutes a system: Documentation, Hardware and Software. That is, a system's configuration represents its functional (performance) and physical (form and fit) characteristics. These characteristics are described in technical documentation, assessed and approved/verified in technical reviews and configuration audits, and achieved in the delivered and accepted product. The CM processes span all SDLC phases and are driven more by program technical and CM events rather than fiscal periodic events. All configuration changes must be controlled to ensure that they are, first cost effective, necessary and safe, and second are properly documented so that all producers, users, and support personnel are aware of their current configuration status.*

The Program Manager (PM) is responsible for the overall conduct of CM and technical data management for the program and will ensure that the following CM objectives are incorporated in business planning, and program planning, execution and support:

- *Functional and physical characteristics of components designated as configuration items (CIs) and associated work products throughout the SDLC, must be identified and documented. The product attributes should be defined, product configurations documented and a basis for making configuration changes established via the usage of configuration baselines. Products are labeled and correlated with their associated requirements, design and product information.*
- *Changes to CIs and their related technical documentation should be controlled. Proposed configuration changes should be identified and evaluated for impact, prior to making change decisions. Configuration change activity should be managed by a formally chartered Change Control Board (CCB) and a defined process for review and approval or disapproval. The PM is typically designated as the CCB Chair, responsible for approval or disapproval of all proposed configuration changes during the acquisition/development and implementation. CCB chair responsibility and authority may be transferred to another activity after the acquisition, development and full deployment completion.*
- *Information needed to manage configuration items effectively, including the status of proposed configuration changes and implementation status of approved configuration changes, must be recorded and reported. The configuration information captured during product definition, configuration change management, product build, distribution and deployment, operation and sustainment, and disposal processes shall be organized for retrieval of key information and relationships, as needed. Configuration information should provide continuous traceability and status of all proposed configuration changes from initiation to implementation or rejection.*
- *The complex aggregate of configuration items must meet the system specified and operational requirements. Actual product configuration should be verified against the required attributes and configuration documentation through functional and physical configuration audits. Incorporation of configuration changes should be verified and recorded throughout the life cycle.*

1.1 Purpose

Describe why this CM plan was created, what it accomplishes, and how it is used. Explain, in simple straightforward terms, the processes required to ensure that the inevitable changes do occur within an identifiable and controlled environment. Mention that the CM plan is intended to be a living document. Consequently, its final version will, itself, be placed under the CM control and the respective changes managed accordingly.

1.2 Scope

- *Define the scope of CM planning.*
- *Define the scope of control – Is this a System/project/Program level artifact?*

- *Provide a high description of the types of artifact that will be placed under CM Control, referencing the CI list.*
- *Identify the systems that are covered under CM control*
- *Identify the process for adding or removing systems from CM control*
- *Unique system characteristics or unique support concepts that require special CM attention;*

1.3 Program Description

Describe the system, its history and the enterprise architecture (EA) under which, the project operates. Identify interface(s) with other legacy or new systems. List the sites that are using the system.

1.4 Reference Documents

The documents listed below are referenced in this CM plan and provide guidance or additional information. The documents may also include additional standards to be followed for CM processes

Required Documents:

- Project Management Plan (PMP)
- Configuration Item List (CI List)

Optional Documents

- *Configuration Management Handbook*
- *Change Control Working instructions*
- *CCB Charter*

1.5 Glossary

Provide definitions for terms and acronyms that appear in the CM plan.

2 CONFIGURATION MANAGEMENT ROLES/RESPONSIBILITIES

Provide a list of the specific groups or individuals involved in the program/project's configuration management activities, and then describe their respective tasks and responsibilities. In some cases, the same individual may perform multiple roles across the organization.

Identify the organization where the CM resides and all other organizational units. Define the functional roles of these organizational units within the project. Describe any internal review and/or Change Control Board. For each board discuss membership (and their functional representatives) and the responsibilities of the board and that of each member.

2.1 CM Responsibilities

Table 2-1 identifies the various CM roles and their corresponding responsibilities.

Role	**Responsibility / Task**
Government Project Manager	▪ Participates in and oversees the configuration management process
Contractor Project Manager	▪ Coordinates CM activities in the project schedule as part of the regular
Project Team	▪ Follows CM Procedures for document management ▪ Implements the required solution for changing and updating code ▪ Updates change control records as part of the documented processes
CM Lead	▪ Production and Maintenance of the project's CMP; ▪ Management of CM organization (responsibilities, authorities, applicable policies, directives and procedures); ▪ Performance of the CM-specific Activities (configuration identification, Change Control, etc); ▪ Handling of the CM Schedules (coordination with other project activities); ▪ Management of the CM Resources (tools, physical, and human resources)
Configuration Control Board	▪ Administering the CM process and approval of software and document baselines ▪ Approving and disapproving change requests to the approved baselines ▪ Prioritizing approved changes for implementation ▪ Ensuring that all requested changes are consistent with current FAS/GSA guidance and requirements

Table 2-1. CM Roles and Responsibilities

3 CM ACTIVITIES

Identify CM activities. Following is a sample listing of CM activities:

- *Governance and Management of the CM processes;*
- *Configuration Identification;*
- *Change Control;*
- *Configuration Status Accounting;*
- *Configuration Auditing;*
- *Build and Release Management.*

3.1 Configuration Identification

Configuration Identification is the basis on which the CIs are defined and verified; CIs and documents are labeled; changes are managed; and accountability is maintained. The sections below define the tools that will be used to track and control the configuration baselines. This section will also describe the methods for controlling, tracking, implementing and reporting changes

3.1.1 Configuration Item Identification

A CI is an aggregation of software, hardware, database, documentation, interface, or discrete portion of hardware or software that satisfies an end-user function and that is designed for control by CM. The selection of CIs is closely coupled with the design process and is determined by the need to control an item's characteristics and its interface with other items. Some of the primary criteria for designating separate CIs include:

- Independent end use functions
- Critical, new, or modified design
- Previously identified as a CI
- Required tracking to the exact configuration and status of changes to the item
- Interface with other systems, equipment, software, or CIs
- Interface with software/hardware developed under another effort
- Separate definition of performance and test requirements
- High risk and critical components
- Separate delivery or installation requirement

The process of selecting CIs requires good systems engineering judgment supported by cost trade-off considerations. There are no fixed rules for selecting or deciding the optimum number of CIs for a particular system. The following identifies some of the problems with identifying too many CIs:

- Excessive development activities including design and verification demonstrations, system integration and testing, technical reviews and budget allocations
- Unnecessary design constraints requiring formal test and technical reviews, beyond what is required to achieve reasonable assurance of the system's performance
- Numerous inter-CI interfaces with little functional impact on the overall system
- Increased overall number of requirements disproportionate to the overall functionality of the system
- Excessive fragmentation of the system which may decrease the visibility and understanding of system performance

On the other hand, having too few CIs introduces another set of problems including:

- Increased development, maintenance, and installation costs because of the increased complexity
- Increased complexity of each CI resulting in decreased insight and ability to monitor progress
- Potential reuse of the CI is diminished
- Formal testing of critical capabilities are made more difficult or require increased time to complete the tests
- Difficulty in addressing the effectiveness of changes

Configuration Item (CI) selection separates system components into identifiable subsets for the purpose of managing further development. It specifies all the components, sub-components, and CIs of an IT system. The most basic function it serves is to identify what comprises the IT system. A CI can be a database, a software module, a specific HW component, an interface, a COTS product, or a system related document.

3.1.2 Configuration Documentation

As part of Configuration Identification, the project team must define the specific technical documentation that will be part of each baseline. The baseline definition is provided in this plan. The documentation required for each successive baseline may be an independent grouping of design information. In some cases, it may be confined to updates to the previous baseline document.

Baseline documentation is maintained and archived in the CM Library (CML). A list of baseline documentation will be maintained to ensure requirements traceability to CIs, baseline specifications, requirements documentation, and acceptance criteria. Documents will be indexed to facilitate retrieval for use, reference, or reproduction.

The project classification schema identifies the minimum required documentation for each project size.

A *partial list of typical documentation includes:*

- *CM Plan*
- *Quality Assurance Plan*
- *Operations Plan*
- *System Security Plan*
- *Project Management Plan*
- *Test Plan*
- *Systems Engineering Management Plan*
- *Functional Requirements Document*
- *Interface Control Document*
- *Security Risk Assessment*
- *System Software*
- *System Design Document*
- *Maintenance Manual*
- *Operations Manual or Systems Administration Manual*
- *Training Plan*
- *User Manual*
- *Test Analysis Report*

3.1.3 Product Structure

Product structure, also referred to as system architecture, defines what constitutes the CI. It refers to the identifiers, internal structure, and relationship of CIs and associated documentation. The product structure may be depicted graphically as a tree structure or as an indented list.

3.1.4 Product Identification

The following principles apply to the identification of CIs:

- All CIs are assigned unique identifiers so that one CI can be distinguished from other CIs; one version of a CI can be distinguished from another; the source (e.g., software, hardware, database, documentation) of a CI can be determined; correct CI information can be retrieved; and the owning system can be determined.
- Individual components (e.g., software files, database files, hardware components) of a CI are assigned unique identifiers when there is a need to distinguish one unit of a CI from another unit of a CI. These individual components are connected to the owning CI.
- When a CI is modified, it retains its original CI identifier even though its part identifying number is altered to reflect a new configuration.

- A series of like components of a CI is assigned a unique CI group identifier when it is unnecessary or impractical to identify individual units but necessary to correlate units to a process, date, event, or test.

The following list identifies the CIs for this <Program/Project> and the corresponding level of Control.

Identify the CIs to be controlled and specify a means of identifying changes to the CIs and related baselines. Identify the rules for including items as CI's.

3.1.5 Naming Conventions

Provide details of the file naming convention to be used on the project and how file configuration integrity will be maintained.

3.1.6 Labeling

Describe the procedures and format for labeling all items under CM control, including code, documentation, and physical media.

3.1.7 Classification Requirements

Describe the rules and documentation standards for classification guidance.

3.2 Configuration Baseline Management

A baseline is a comprehensive set of CIs (products, deliverables) developed during a specific phase of the development process that has been formally accepted. The baseline, usually tracked through a label or version, should incorporate all artifacts at that stage in the SDLC, to include, documents, code, and plans. Once the baseline is established, changes to the CIs can only be done through a formal change process, as documented in this plan. Baselines may also be established to signify the progress of work through passage of time. In this case, a baseline is a visible stake through an endured collective effort, e.g. a developmental baseline.

Define the baselines that will be created, the required artifacts/elements for each baseline and the trigger for the creation.

Figure 3-1 is a representative sample of various baselines:

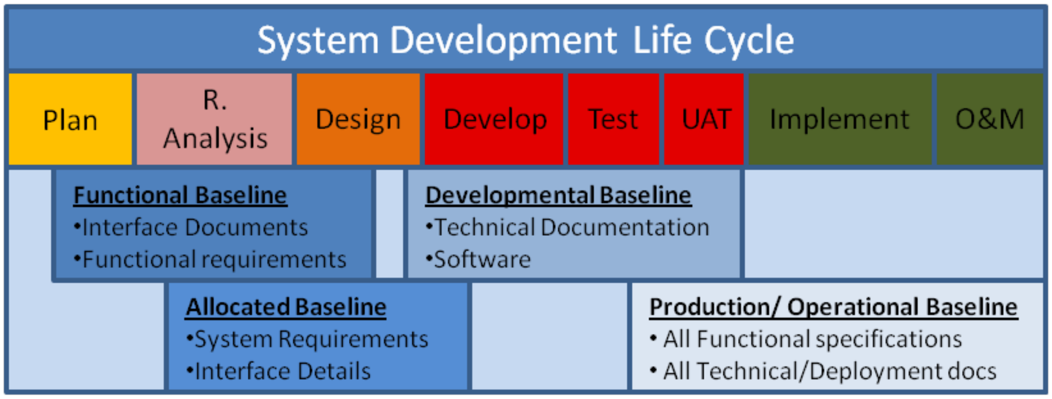


Figure 3-1. Baselines and Mapping to SDLC Phases

3.2.1 Functional Baseline

The functional baseline is established by the system specification or equivalent. It describes a system's or top level CI's functional, inter-operability, and interface characteristics and the verification required to demonstrate the system or CI meets these characteristics.

The functional baseline is normally established at the end of the system concept development phase. This initial baseline will be developed based upon the functional requirements. After system requirements review, additional information may be added. This baseline is subject to CM control.

The functional baseline is established by the system specification or equivalent. It describes a system's or top level CI's functional, inter-operability, and interface characteristics and the verification required to demonstrate the system or CI meets these characteristics.

The functional baseline is normally established at the end of the system concept development phase. This initial baseline will be developed based upon the functional requirements. After system requirements review, additional information may be added. This baseline is subject to CM control.

3.2.2 Allocated Baseline

The allocated baseline describes the functional and interface characteristics that are allocated from those of the higher lever CI and the verification required to demonstrate the CI meets these characteristics. The allocated baseline is established when a new development specification is authenticated. Authentication should take place before the preliminary design review. The allocated baseline is normally established at the end of the validation phase or at the beginning of the full-scale development phase.

3.2.3 Developmental Baseline

The development configuration is the design and associated technical documentation that defines the evolving design solution during development of the CI. The development configuration for a CI consists of internally released technical documentation for hardware and software that is under configuration control.

The Developmental Configuration may be subdivided into additional environments as required including Development, Integration Test, and Quality Assurance Test.

3.2.4 Production/Operational Baseline

The production/operational baseline is the approved technical documentation which describes the configuration of a CI during the production, fielding/deployment and operational support phases of its life cycle. The product baseline for a CI consists of all necessary physical or functional characteristics of a CI; selected functional characteristics for production acceptance testing; and production acceptance test requirements.

This section should be updated as more detailed information becomes available during the development and deployment of a new or modified system/equipment. Describe what baselines are to be established. Explain when and how they will be defined and controlled.

3.3 Change Control

Change control is systematic proposal, justification, evaluation, coordination, approval and implementation of changes after the formal establishment of a configuration baseline. The process ensures that all changes are authorized, documented and coordinated.

Here, you can identify any provisions for establishing and maintaining configuration traceability to requirements. Describe the change control process. Reference the governing body that approves changes to the baselines.

3.3.1 Change Management

The goal of a change management process is to:

- *Predict and recognize changes*
- *Evaluate and understand the consequences of implementing the proposed changes*
- *Ensure that every propose change is evaluated, reviewed and [dis]approved at the proper authority level*
- *Control the consequences of the approved changes*
- *Prevent unauthorized and unintended deviations from the approved baselines*
- *Ensure that every approved change is documented, tested, verified and, then implemented.*

Define the mechanism(s) for initiation (proposal) and the processes for controlling, changes to the system baselines and for tracking the implementation of those changes. Provide a table listing the roles of the CCB the membership and the way it deals with change initiation, application and control. If appropriate, a separate CCB charter may be referenced.

If a program is a larger size, there may be a need for additional CCB layers to review and approve changes for individual projects and project phases. For example, the program CCB may be responsible for approving all scheduled work while a project level CCB is only responsible for reviewing and approving development/test cycle issues. For the largest programs, an additional layer may be required to review and prioritize issues that cross organizational boundaries or have cross-cutting impacts.

Table 3-1 shows the CCB roles and corresponding responsibilities.

Role	Responsibility / Task
CCB Chair	▪ Schedules the CCB meetings in accordance with organizational policy and schedule requirements
CCB Member – Contractor	▪ Document all proposed changes, ensuring sufficient information and analysis is available for review and approval ▪ Provide technical analysis and review of proposed changes
CCB Member – Government (CIO and Business Line Representatives)	▪ Attend meetings to review proposed changes ▪ Provide advice and approval for documented changes ▪ Ensuring that all requested changes are consistent with current FAS/GSA guidance and requirements ▪ Prioritize approved changes for implementation
CCB Recorder	▪ May be any designated team member, responsible for recording and documenting decisions of the CCB meeting ▪ May be authorized to update the SCR repository with the approved changes
CM Manager	▪ Ensures that SCR data can be provided consistently to the CCB membership ▪ Verifies that the approved changes are properly recorded
Contractor Project Manager	▪ Advisory member of the CCB
Government Project Manager	▪ Voting member of the CCB
Project Team	▪ Advisory members of CCB as needed ▪ Should include members from all phases of the SDLC ▪ Updates change control records (SCR) as part of the documented processes

Table 3-1. CCB Roles and Responsibilities

3.3.2 Communications

Document the communication channels and responsibilities. Table 3-2 lists the communication needs, purpose, frequency, and the audience. Pay particular attention to teams and organizations outside of the project/program

Communications	Purpose	Frequency	Audience
Communications Mechanism	Describe its purpose	Weekly / Biweekly / Monthly	Project Team, Project Board, Client
Report Name	Describe its purpose	Weekly / Biweekly / Monthly	Project Team, Project Board, Client
Report Name	Describe its purpose	Weekly / Biweekly / Monthly	Project Team, Project Board, Client

Table 3-2. Communications Description

3.4 Configuration Status Accounting

Configuration Status Accounting (CSA) is process of recording, storing, maintaining, coordinating and reporting the information necessary for the CM performance and the status of its associated CIs. All software and related documentation are tracked from initial development to request for change, through the [dis]approval of changes, to the implementation of changes. Results and decisions of the Change Management process are a key input to a CSA Report (CSAR)

Identify what CSA tools will be used and who will maintain them. Whenever possible, automate the CSA process.

3.5 Configuration Auditing

Configuration audits are comparisons of a product's actual functional and physical characteristics with the characteristics identified in configuration baseline documentation. They verify that the configuration identification for a configured item is accurate, complete, and will meet the specified program needs.

There are two types of audits and they both must be satisfactorily completed as a prerequisite to establishing the product baseline:

- ***Functional Configuration Audit (FCA****) – To be conducted on the first prototype item produced to compare the functional characteristics with the* ***Functional*** *and* ***Allocated*** *baseline information.*
- ***Physical Configuration Audit (PCA)*** *– To be conducted on the first production representative item to compare the physical characteristics with the* ***Product*** *baseline. Discrepancies between the actual configuration and baseline documentation need to be resolved.*

Identify the plans and mechanics to accomplish these audits. Describe how the peer reviews and formal audits will be accomplished. These formal audits may include baseline, functional, physical, software and hardware physical configuration, and subcontractor configuration audits.

4 BUILD & RELEASE MANAGEMENT

Dedicated to the release of an executable version of a software product, this CM activity orchestrates the complex assembly, verification and packaging processes that produce the executable. To achieve this, the correct baseline, composed of baseline versions of CIs, is compiled (built) into an executable. Since the executable represents the only true record of what development delivers to customers, build and release management provides the essential link between development output and what is ultimately deployed into production.

Once an executable is created, it should be delivered for testing or distribution to the customer. Specific build instructions are needed to guarantee that the build steps are taken and that they are performed in the correct sequence. Sometimes different versions of the same product should be built (for platform, customer, functionality, etc.)

4.1 Libraries

Identify the documentation control parameters (including the responsibility for them,) control libraries and media (if applicable) and how the access control is to be managed.

4.2 Automated Tools

Describe any automated case tools used and the processes used for their source control.

4.3 Version Control

Describe the processes for controlling the amount and number of versions documented by this CMP.

4.4 Build Management

Describe the controls in place to manage the building of executable code.

4.5 Version Description Document

The VDD is the primary configuration control document output of the build process. It is used to track and control versions of software being released to testing or to final implementation, The VDD provides a summary of the features and contents for a specific software build or release, and facilitates product implementation, testing, operations and maintenance. The VDD identifies and describes the version of the configuration items (CIs) that comprise the software build or release, including all changes to the CIs since the last VDD was issued, as well as installation and operating information unique to the version described. The VDD applies to any release of a product revision, and includes software, hardware, and firmware.

5 REVIEWS

All baseline operational components (including the support documentation), are subject to a final review (i.e., Users' Manual, Computer Operations Manual, etc.....) for conformance to the initial design.

Describe how the technical reviews relate to the establishment of baselines and explain the role of CM in these reviews.

6 CONFIGURATION MANAGEMENT MEASURES

Describe the metrics that will be used to measure CM activities. Sample metrics include:

- *Planned vs Actual builds*
- *Number of emergency releases*
- *Number and size of repositories under control*
- *Number of approved and unapproved changes by the CCB*

Quality Assurance Plan *(QAP)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

QUALITY ASSURANCE PLAN

Executive Summary

Quality Assurance Plan (QAP) presents a framework for potential activities, which when followed, will ensure delivery of quality products and services. This QAP document, is applicable at two levels of:

- Program (pQ) detailing the activities that QA could apply to a task as it goes through the life cycle;
- Project (tQ) describing the actual QA activities that will be integrated with the project plan and schedule. The level of detail for tQ(s) should be consistent with the complexity, size, intended use, mission criticality, and cost of failure of the development effort.

1.0 OVERVIEW

1.1 Purpose

The purpose of the QAP is to ensure that delivered products satisfy contractual agreements, meet or exceed quality standards and comply with approved SDLC processes.

1.2 Scope

Describe the scope of the QAP as it relates to the project.

1.3 System Overview

Provide a system overview as a reference point for remainder of the document, including the project's quality objectives as established by the Project Manger (**PM**), the responsible organization, operational status, system environment and special conditions. Also describe the benefits that will be realized by conforming to quality requirements and the contributions that QA makes to the success of the program.

1.4 Project References

List all project-specific documentations and all the standards that govern the FAS' QA function.

1.5 Glossary

Provide definitions for terms and acronyms used within the QAP.

2.0 ORGANIZATION

Provide the following organizational information:

- An organization chart (preferably from a *QA perspective*)
- Organizational and functional alignment of the QA staff including their roles and responsibilities
- Tasks in terms of QA activities associated with the project
- A list of organizations that require coordination between project and its specific support function (*e.g.,* linkage between QA and development, configuration management (CM), security, testing & evaluation, *etc.*). Include a schedule for coordination activities
- A list of points of contact (POCs) that may be needed by the document user for informational and troubleshooting purposes.

3.0 PROCESSES

Detail the processes used by the QA uses to ascertain that processes and products associated with hardware, software, and documentation are monitored, sampled, and audited to verify compliance with the FAS' established methodology, policy and standards.

3.1 General

Describe QA's role in performing reviews and audits associated with work products and with collections of work products making up an SDLC phase.

3.2 Peer Review

Describe the QA participation in the peer review process to identify, document, measure and eliminate defects in a work product.

3.3 Process Review

Describe the audit and assessment reviews that ensure that appropriate steps are taken to carry out activities specified by the SDLC. Describe methods by which QA monitors processes by comparing the actual steps taken with those in documented procedures. Discuss the QA' responsibility of informing the management (with the help of review results data,) of the project's actual progress, status and quality.

4.0 PROBLEM REPORTING AND CORRECTIVE ACTION

Detail QA' role in identifying problems and recommending corrective actions. Discuss procedures and formats for preparation, tracking and management involvement in the use of project specified problem reporting forms/mechanisms.

4.1 Home-Grown Problem Reporting Forms (Action Reports)

Describe preparation of project specified problem reporting forms to document anomalies, violations of program standards, or potential problems as identified during a point in SDLC (including the formats.)

4.2 QA Escalation Procedure

Describe the QA escalation procedures that bring high-risk or long-standing, unresolved noncompliance issues to the senior management's attention.

5.0 TOOLS, TECHNIQUES, AND METHODOLOGIES

Identify tools, techniques and methodologies used by QA. Discuss the application of these items to the QA function in appraisal, preventive (nonconformance identification) and corrective actions.

5.1 SDLC

Describe QA's use of the SDLC, supporting policies and accepted standards in management of internal activities, as well as, ensuring the same for all contractors.

5.2 Policies

Describe QA's role in developing policy statements that expand, enhance or clarify SDLC requirements, as well as introducing new or enhanced standards.

5.3 Standards

Detail the QA requirement of ensuring that there exist standards that establish the prescribed methods for development of work products. Discuss QA's role in assessing standards for adequacy/applicability.

5.4 Tools

Describe the tool sets that QA employs in the conduct of administrative and technical functions.

Concept of Operations *(ConOps)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

CONCEPT OF OPERATIONS

Executive Summary

An organization develops a Concept of Operations (ConOps) document to establish the desired system approach that it wishes to take. The ConOps service works with organizations to document decisions that define the approach and the organizational structure needed to put the approach into operation.

The ConOps is, then, a user-oriented document that describes system characteristics for a proposed system from the users' viewpoint. It is used to communicate overall quantitative and qualitative system characteristics to the user, buyer, developer and other organizational elements. ConOps also defines the user organization, mission and organizational objectives from an integrated systems point of view.

1.0 OVERVIEW

1.1 Purpose

Describe why this ConOps document was created and what it accomplishes. The intended audience for the ConOps should also be described. The audience can be a variety of people with various levels of technical knowledge. Therefore, it is important that ConOps be clearly written to clearly define technical terms and utilize layman English for the majority of the text. In short, the purposes of a ConOps will be:

- To communicate user needs and the proposed system expectations
- To communicate the system developer's understanding of the user needs and how the system will meet those needs

1.2 Scope

Provide an estimate of the size and complexity of the system.

1.3 System Description

Provide the purpose of the proposed system or subsystem to which the ConOps applies. Describe the general nature of the system, and identify the project sponsors, user agencies or departments; system developers; maintenance and support entities; evaluation and certification entities; and the operating centers or sites that will run the system.

A high-level graphical overview of the system is strongly recommended. This can be in the form of a physical layout diagram, top-level functional block diagram, or some other type of diagram that depicts the system and its environment. Documentation that might be cited includes, but is not limited to, project authorizations, relevant technical documentation, significant correspondence, risk analysis reports and feasibility studies. If applicable, identify interface(s) with other legacy or new systems.

1.4 Reference Documents

Detail all the documentations referenced in the ConOps document. Include meeting summaries, white paper analyses, SDLC work products, as well as any other related documents.

1.5 Glossary

Provide definitions for terms and acronyms used in the ConOps. This may be provided as an appendix.

2.0 THE CURRENT (AS-IS) SYSTEM

This section of ConOps describes the problem to be solved, and the system or situation as it currently exists. Here, you should first answer the following questions:

- What is the system?
- What is the system supposed to do?
- Who owns, operates, and maintains the system?
- How well does the system perform?
- What is the system's geographic coverage?
- When is the system used?
- How does the system operate?
- What other systems does it talk to?

If there is no current system, describe the reasons and motivations for developing the proposed system. Introduce the problems, needs, issues and objectives that must be addressed by the proposed system. This enables the reader to better understand the reasons for the desired changes and improvements.

2.1 Description of the Current Situation

Provide a thorough description of the current system, including operational characteristics; major system components; component interconnections; external interfaces; diagrams illustrating inputs, outputs, and data flows; system costs; and performance statistics. Include description of the users and other people who interact with the system (i.e., responsibilities, skill levels, work activities, etc.)

2.2 Support Environment

Describe how the system is supported and maintained, including facilities; equipment; support software or hardware; and repair or replacement criteria. Identify whether the system will be maintained by *FAS FTEs* or a vendor will be contracted to maintain the system.

2.3 Users Information

Explain how the users interact with the system and the scenarios that occur when they interact with the system. Discuss how the users interact with each other. For example, a supervisor user class may have certain capabilities that an operator class may not have with the system, and the ConOps should describe when, why, and how such an interaction takes place to achieve a system objective or function.

2.4 Operational Constraints

Describe limitations on the operational characteristics of the system. This could include limits on hours of operation, hardware limitations or resource limitations.

3.0 JUSTIFICATIONS FOR THE PROPOSED (TO-BE) SYSTEM

Detail the shortcomings of the current system or situation that motivate development of the *proposed* system. If the goal is to make modifications to the current system, describe the nature of the desired capabilities along with the *expanded* mission, objectives and scope.

3.1 Reasons for the Desired Changes

Present the reasons for developing the proposed system, including:

- Limitations, shortcomings and/or dependencies of the current system;
- New Mission;
- New or modified user needs;
- New objectives.

Fortify the argument by defining the goals and objectives of the new system and the business problems that it will rectify.

3.2 Description of the Desired Changes

Summarize the new and/or modified capabilities, functions, processes, interfaces and other changes needed to respond to the justifications previously identified:

- Capability Changes - functions and features to be added, deleted or modified;
- Environmental Changes - changes in the operational environment;
- Interface Changes - changes in the system that will cause changes in the interfaces and changes in the interfaces that will cause changes in the system;
- Operational Changes - changes to the user’s operational policies, procedures or methods;
- Other Changes that will impact the users;
- Personnel Changes - changes in personnel caused by new requirements;
- Support Changes - changes in the support or maintenance requirements;
- System Processing Changes - changes in the process or processes of transforming data that will result in new output with the same data, the same output with new data or both.

3.3 Change Priorities

Present prioritization or ranking regarding the proposed changes. Define what features are essential, what features are desirable and what features are optional.

3.4 Excluded Changes

Detail the significant changes or features that were assessed but not included in system description. This information is included to assist others in knowing what other options were considered and why they were not included.

3.5 Assumptions

Describe assumptions or constraints applicable to the changes and new features identified. Include all assumptions and constraints that will affect users during development and operation of the proposed or modified system.

4.0 FUNCTIONAL REQUIREMENTS FOR THE PROPOSED (TO-BE) SYSTEM

Describe the proposed system that derives from the changes specified in the previous section. Include a high level description of the new system that presents the operational features, without specifying design details. This level of detail should be sufficient to fully explain how the proposed system is envisioned to operate in fulfilling user needs and requirements. In the event that actual design constraints need to be included in the description of the proposed system, they shall be explicitly identified as requirements to avoid possible "misunderstandings."

In summary, describe the following for the proposed system, at the high level:

- Background, objectives and scope
- Capabilities, features and functions
- Major components
- User involvement and interactions
- Support environment
- External interface (including the inbound/outbound data) requirements
- Modes of operations (Normal and Emergency)
- Geography and climatology (if applicable)
- Interoperability requirements (both internal and external)
- Critical Technical Parameters and Operational Policies/Issues

Detail each major process and the functions or steps performed during each work process. State the processes and functions in a manner that enables the reader to see broad concepts decomposed into layers of increasing detail. Then show, in a diagram, the sequence of process steps described above high-level functional requirements.

4.1 The Proposed System Capabilities in Detail

Describe the system operational capabilities necessary to satisfy mission performance requirements. A thorough description of the proposed system should be provided that includes:

- Characteristics of Operational Environment and Performance
- Major system components and the interconnections among these components
- Interfaces to external systems or procedures
- Relationship to other systems
- Conformity and Compatibility with the established GSA and FAS standards
- Cost of system operations
- Deployment and operational risk factors
- Provisions for safety, security, privacy, integrity, and continuity of operations in emergencies
- Quality Attributes:
    - accuracy,
    - availability,
    - expandability,

- flexibility,
- interoperability,
- maintainability,
- portability,
- reliability,
- reusability,
- supportability,
- survivability,
- usability

Since the purpose of this section is to describe the proposed system and how it should operate, the system description should be simple and clear enough that all intended readers can fully understand it. It is important to keep in mind that the ConOps should be written in the user's language. Graphics and pictorial tools should be used wherever possible. Useful graphical tools include, but are not limited to, the contract work breakdown structure (CWBS); sequence or activity charts; functional block diagrams; and relationship diagrams.

The operational environment description should identify the facilities, equipment, computing hardware, software, personnel and procedures needed to operate the proposed system. This description should be as detailed as necessary to give the readers an understanding of the numbers, versions, capacity, etc., of the operational equipment to be used.

The ConOps author(s) should organize the information for the proposed system in such a manner, that a clear picture of the proposed system is painted. If a part of the description prove to be voluminous, it can be included in an appendix or incorporated by reference. An example of material that might be included in an appendix would be a data dictionary. An example of material to be included by reference might be a detailed operations or policy manual.

5.0 OPERATIONAL SCENARIOS

A scenario is a step-by-step description of how the *proposed* system should operate and interact with its users and its external interfaces under a given set of circumstances. Scenarios are written in layman's language and should be as non-technical as possible. They should be described in such a way that will allow readers to walk through them and gain an understanding of how the various parts of the *proposed* system function and interact. Scenarios may also be used to describe what the system should not do.

Scenarios should be structured to describe a specific operational sequence that depicts the role of the system and its interactions with users and other systems. Operational scenarios are to be described for all operational modes of the *proposed* system. Each scenario should include information, events, actions, inputs and interactions, to provide a clear understanding of the operations of the *proposed* system.

It is necessary to develop several variations of each scenario, including one for normal operation, one for exception handling, one for degraded mode operation, etc.

Scenarios play several important roles:

- They bind all individual parts of a system into a comprehensible whole and help the readers of a ConOps document to understand how all the pieces interact to provide operational capabilities
- They provide readers with operational details for the proposed system, thus, enabling them to understand user roles, how the system should operate and the various operational features
- They can serve as the basis for the first draft of a users' manual and as the basis for developing acceptance test plans to verify that the system design will satisfy user needs and expectations.

Creative writing and graphics should be employed to make the scenarios interesting and easy to read. A good ConOps must have a story line that features different characters that relate to the environment and situation where the proposed system is being contemplated and a common thread weaving through all the characters as they interact with the system. Story lines should also highlight key features based on the initial understanding of the problem to be solved and user needs so that readers can understand the consequences of their needs when they are translated to a system that will satisfy those needs.

Scenarios are important components of a ConOps and, therefore, should receive substantial emphasis. The number of scenarios and level of detail specified will be proportional to the complexity and criticality of the project.

6.0 SUMMARY OF IMPACTS

Describe and summarize the operational impacts of the *proposed* system from the users' perspective. Here, also include a description of the temporary impacts that can be realized during the development, installation or training periods. This information is provided to allow all affected departments to prepare for changes that will be brought about by the new system, and to allow those divisions/departments or other agencies to plan for the impacts including operational, organizational and developmental impacts.

7.0 ANALYSIS OF THE PROPOSED SYSTEM

Provide a summary of the benefits, limitations, advantages, disadvantages, alternatives and trade-offs considered for the proposed system. Improvements to the system should be documented. This includes a qualitative and quantitative summary of benefits of implementing the proposed system, and can include improved performance, new/enhanced and/or deleted capabilities and any disadvantages or limitations.

Also, all the major alternatives1, the tradeoffs amongst them and the rationale for the decisions reached must be summarized. This information is useful in determining whether an approach was analyzed and evaluated or why a particular approach or solution was rejected.

Present the rough order of magnitude (ROM) cost figures for the proposed system based on clearly stated assumptions. A tentative development schedule should also be included in this section.

[1]: The term *alternatives* here, means the operational, and not the design, alternatives. Except to the extent that the design alternatives may be limited by the operational capabilities desired in the *proposed* system.

8.0 NOTES

Any additional information that will aid in understanding the ConOps, should be documented here. Even if there are no notes, this section should still be included with the notation that there are no notes at this time. Subsequent revisions of the ConOps usually require that notes be added.

9.0 APPENDICES

To facilitate the ConOps' ease of use and maintenance, the information on studies or other analytical activities conducted thus far, may be placed in appendices. Each appendix should be referenced in the main body of the document where that information would normally have been provided. Appendices may be bound as separate documents for easier handling.

Systems Engineering Management Plan *(SEMP)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	

SYSTEM ENGINEERING MANAGEMENT PLAN

EXECUTIVE SUMMARY

The system engineering management plan (SEMP) is the vehicle that documents and communicates the technical approach including the application of the common technical processes; resources to be used; the key technical tasks, activities, and events along with their metrics and success criteria. SEMP communicates the technical effort that will be performed by an assigned technical team to the team itself, managers, customers and other stakeholders. Whereas the primary focus is on the applicable phase in which the technical effort will be done, the planning extends to a summary of the planned technical efforts for future applicable phases.

The primary function of SEMP, therefore, is to provide the basis for implementing the technical effort and to communicate:

- What will be done;
- Why is it being done;
- Who is going to do it;
- When is it going to be done; and
- Cost (and the cost drivers).

It also identifies the roles and responsibility interactions of the technical effort and how those interactions will be managed.

1.0 OVERVIEW

1.1 Purpose

Describe why this SEMP document was created and what it accomplishes. State that SEMP is a "living" and tailorable document that captures a project's current and evolving systems engineering strategy and its relationship with the overall project management effort throughout the SDLC.

The SEMP's purpose, then, is to guide all technical aspects of the project. The intended audience for the SEMP should also be described.

1.2 Benefits Statement

Provide the perceived benefits of developing the SEMP. The following can be used as examples:

- Provides modern, state-of-the-art, project management guidance for the design, development, evaluation, production, evaluation, and maintenance of technical systems;
- Limits and reduces the proliferation of management documentation and implements relevant aspects of international standards;
- Provides a coherent view in pursuance of joint international requirements;
- Identifies relevant directives and references;
- Establishes a relationship with international standardization specifications (if applicable);
- Provides evidence that control over the design, development, production, installation and support will be performed;
- Provides emphasis on a disciplined integrated systems development approach;
- Familiarizes the newcomers with the concepts of systems engineering management and techniques;
- Provides visibility and communication of Engineering Management. It is crucial that doing the design and development phase, those questions are asked and answers are given; only in this way is it possible to integrate complex systems, learn from the past mistakes and successes and feed-forward problems for which timely solutions must be found.

1.3 Scope

Provide an estimate of the size and complexity of the system. Where applicable, tailor the scope to fit the statement of work (SOW) used by both the acquirer and design authority for the effort.

1.4 Reference Documents

Identify all the applicable and referenced documents which are required for the specific program or project, as well as, any contractual and non-contractual provisions. Also, state the order of precedence and availability of the documents.

1.5 Glossary

Provide definitions for terms and acronyms used in the SEMP. This may be provided as an appendix.

2.0 TECHNICAL PROGRAM PLANNING AND CONTROL

First, describe the project to include complexities and challenges that are addressed by the technical development. Then identify the organizational responsibilities and the authority for system engineering management, including control of subcontracted engineering:

- Levels of control established for performance and design requirements and control of the method used;
- The technical program assurance methods;
- Plans and schedules for design and technical program reviews;
- Control of documentation;
- Design approval and certification;
- Transfer of information from paper to electronic media (if applicable).

3.0 SYSTEM ENGINEERING PROCESS

Detail the system engineering process to be used and the specific organizational responsibilities for the technical effort (including [sub]contracted technical tasks.) Reference all the technical processes and procedures to be used (if any) and their need dates and development schedule(s):

- Procedures to be used in implementing the process;
- In-House Documentation;
- Trade Study Methodology;
- Mathematical and/or Simulation models to be used;
- Generation of Specifications.

3.1 Systems Engineering Process Planning

Present planning for the key system outputs to include products, processes and trained people. The following can be used as example:

- Major Products. Include major specification and product baseline development and control
- System Engineering Inputs. Include major requirements documents and resolution instructions for conflicting requirements
- Technical Objectives. Include cost, schedule, and key performance objectives
- Work Breakdown Structure. Detail how and when a WBS will be developed
- Subcontracted Technical Efforts. Describe the integration of contracted and subcontracted technical efforts
- Processes. Describe the use of established technical processes and standards on the project
- Process Development. Describe processes to be developed as part of the project, together with their development schedule
- Constraints. List any significant constraint to the technical effort

3.2 Mission Requirements Analysis

Discuss the SEMP system's operational characteristics, mission, threat, environmental factors, minimum acceptable functional requirements and technical performance.

3.3 Functional Analysis

The system capabilities and states and modes of the system must be progressively identified/analyzed as the basis for identifying alternatives for meeting the system performance and design requirements.

Every capability function and sub-function, should then be allocated a set of performance and design requirements. These requirements are to be derived concurrently with the development of capabilities, time-line analyses, synthesis of system design, and evaluation performed through trade-off studies and system/cost effectiveness analysis.

3.4 Synthesis

Describe the system's performance, configuration and arrangement of its elements and the techniques for test, support and operation.

This description can be supplemented by physical/mathematical models, schematic diagrams, computer simulations, layouts, detailed drawings, [data]flow diagrams, hierarchical objects and similar engineering graphics. These schematics should depict intra- and inter-system and item interfaces, permit traceability between elements at various levels of detail and provide the means for complete and comprehensive change control.

3.5 System Analysis

Detail the processes and procedures to be used for formal and informal trade studies, to include system and cost-benefit effectiveness analyses and the risk management approaches.

3.6 System Control

Provide detailed control strategies needed for the following:

- Configuration Management
- Data Management
- Formal Technical Reviews
- Informal Technical Reviews/Interchanges
- Interface Management
- Quality Assurance (and Control)
- Requirements Control
- Schedule Tracking and Control
- Subcontractor/Supplier Control
- Technical Performance Measurement.

4.0 SPECIALTY ENGINEERING INTEGRATION

Detail the integration and coordination of the efforts for engineering specialty areas. To achieve a best mix of the technical/performance, the values incorporated in the contract must be described with the detailed specialty program (project) plans being summarized and/or referenced, as appropriate.

Specialty efforts and parameters that are to be integrated into the system engineering process at each iteration, should be described and their considerations defined.

5.0 TECHNOLOGY REFRESHMENT

Describe the plans to establish and maintain a viable technology baseline during project development. Also discuss the strategy to be used during development to ensure refreshment remains a viable option in the future project operations.

6.0 NOTES

Any additional information that will aid in understanding the SEMP, should be documented here. Even if there are no notes, this section should still be included with the notation that there are no notes at this time. Subsequent revisions of the SEMP usually require that notes be added.

Functional Requirements Document

(FRD)

(Version 1.1)

[Program/Project Name]

Federal Acquisition Service (FAS)

mm/dd/yyyy

March 1st, 2012

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006
Version 1.1	Broke out the requirements traceability matrix (RTM) as a separate document	March 1st, 2012

EXECUTIVE SUMMARY

A requirement is a need that **must** be satisfied. It ideally:

- Provides a benefit that is directly traceable to the business objectives and business processes in an organization's strategic plan
- Describes the capabilities the application must provide in business terms
- Describes neither how the application provides those capabilities, nor any design considerations
- Is stated in unambiguous words. Its meaning is clear and understandable
- Is verifiable.

Once the stated requirements are collected, they are classified, sorted and organized in what is called a functional requirement document (FRD). As a system's de-facto requirements repository, FRD is a formal statement documenting an application's functional requirements and has the following characteristics:

- It demonstrates that an application provides business value to an organization according to the processes and objectives put forth in the organization's strategic plan
- It contains a complete set of requirements for the application. It leaves no room for anyone to assume anything not stated in the FRD.
- It is *solution independent*. Though, it does specify what the application is supposed to do, it does not say how the application works, nor does it commit the developers to a particular design. For that reason, any reference to the use of a specific technology is entirely inappropriate in an FRD.

1.0 OVERVIEW

Planners state most requirements in functional terms, leaving the design and implementation details to the developers. Sometimes the requirements are described more precisely than realistically, creating a situation where, according to Kaner, Falk, and Nguyen:

> ***"A mismatch between the program and its specification is an error in the program if, and only if, the specification exists and is correct. A program that follows a terrible specification perfectly is terrible, not perfect."***

Therefore, in gathering and recording requirements, the following conditions must be paid attention to:

- Are these the "correct" requirements?
- Are they complete, compatible, achievable, reasonable, AND most importantly, testable?

1.1 Project Description

Provide a brief overview of the project.

1.2 Purpose

Describe why this FRD was created and what it does accomplish. Include the business objectives and business processes from the ConOps and the CBA document that this FRD supports.

1.3 Assumptions and Constraints

Assumptions are future *(beyond control)* situations and their outcomes will influence a project's success. The following are examples of assumptions:

- Availability of Hardware/Software Platform
- Pending (*future*) Court Decisions
- Pending Legislation
- Technology Adavances

Constraints are conditions outside the control of a project that limit the design alternatives. The following are examples of constraints:

- Economy (*funding*)
- Government Regulations
- Mandatory Standards
- Strategic Decisions

There also exists *preference*. Also known as *"wish-list items",* preferences should be distinguished from constraints. While constraints do exist because of real business conditions, preferences are arbitrary. For example, a delivery date is a constraint only if there are real consequences for not having met the date. Otherwise, the mere desire to deliver a product on an arbitrarily delivery date is a preference.

Describe any assumptions and constraints that will affect development and operation of the system. Identify any limitations affecting the desired capability, any *preferences* that will not be provided by the system, as well as any anticipated operational changes that will affect the operation of the system.

1.4 External Interfaces

Name the applications with which the subject application must interface. For every interface identified, provide the application's name, owner and detailed interface information.

1.5 Reference Documents

Name the documents that were sources of this version of the FRD. Include meeting summaries, white paper analyses, CBA, ConOps, SDLC work products, as well as, any other documents that contributed to the FRD. Include the CM identifier and date published for each document listed.

1.6 Glossary

Provide definitions for terms and acronyms used in the FRD. This may be provided as an appendix

2.0 FUNCTIONAL REQUIREMENTS

Functional requirements describe the core functionality of a system and consist of functional processes and data requirements.

2.1 Functional Process Requirements

Process requirements describe what the application must do. They may be expressed using text, data flow diagrams or any technique that provides information about the processes performed by the application.

Present the functional process requirements in a manner that enables the reader to see broad concepts decomposed into layers of increasing detail:

- **Access to Stored Data**
- **Context**
- **Data Attributes** *(Input to and Output from the processes)*
- **Detailed View** *of the processes*
- **Failure Contingencies** *(Backup, Degraded Modes of Operation and Fall-Back procedures)*
- **Logic** used inside the processes to manipulate data
- **Processes Decomposed** into finer levels of detail.

2.2 Data Requirements

While describing the business data needed by the system, data requirements do not design a physical database. Describe data requirements by producing a logical application data model that includes entity relationship diagrams, entity definitions and attribute definitions.

3.0 SPECIFIC PERFORMANCE REQUIREMENTS

State performance requirements in a non-business fashion. Do not elaborate on how these requirements will be satisfied. For example, when answering the "What is the minimum acceptable level of reliability?" question, do not elaborate what steps will be taken to provide reliability.

3.1 Audit Trail

Describe all user requirements for an audit trail, such as total transactions processed by location, time, type and retention periods. List the activities that will be recorded in the application's audit trail and for each activity, list the data to be recorded. This should be consistent with the functional requirement for user accountability.

3.2 Capacity

Specify maximum number of transactions, storage requirements, concurrent users or other quantifiable information about the system's capacity requirements. Identify changes to the capacity limits resulting from varying modes of operation. Include peak load limits and issues. Do not state capacities in terms of system memory requirements or disk space.

3.3 Data Currency

Data currency is a measure of how recent your data is. For every data type, answer this question: "When the application responds to a request for data how current must those data be?"

3.4 Data Retention

Provide the length of time the data is required to retained.

3.5 Fault Tolerance

Fault tolerance is the ability to remain partially operational during a failure. Most applications, do not have fault tolerance requirements. However, *when applicable*, describe:

- Which functions need not be available at all times?
- If a component fails, what functions must the application continue to provide?
- What level of performance degradation is acceptable?

3.6 Performance

Present the requirements for the following:

- Expected Data Volume
- Expected User Activity Volume *(for example, number of transactions per hour, day, or month)*
- Response Times:
  - From receipt of request to availability of system products
  - For Queries and Updates
  - Sequential Relationship of Functions
  - Priorities imposed by Input Types and Changes in Modes of Operation
  - Any deviations from specified response times for peak load periods or contingency operations.
- Throughput.

3.7 Recoverability

Recoverability is the ability to restore function and data in the event of a failure. Answer the following:

- If a system goes down (application becomes unavailable) due to a failure, how soon must it be restored?
- If the database gets corrupted, to what level of currency must it be restored?
- If the site (hardware, data and onsite backup) is destroyed, how soon must the application be restored?

3.8 Reliability

Reliability is the probability that the system will be able to process work correctly and completely without being aborted. Address the following:

- What damage can result from this system's failure?
  - Complete or Partial Loss of the ability to perform a mission-critical function
  - Loss of employee productivity
  - Loss of Human Life
  - Loss of revenue.

- What is the minimum acceptable level of reliability? Respond in any of the following ways:

Benchmark	Computation
Mean Time Between Failure	The number of time units the system is operable before the first failure occurs
Mean Time To Failure	The number of time units before the system is operable divided by number of failures during the time period
Mean Time To Repair	The number of time units required for system repair divided by number of repairs during the time period

3.9 Security

Discuss the need to control access to the data in order to maintain its confidentiality, availability and integrity. This includes controlling who may view and/or alter data within the system.

3.9.1 Breaches

Explain the consequences of the following breaches of security in the subject application:

- Contamination or Erasure of Application Data
- Disclosure of Government Secrets
- Disclosure of Privileged Information about Individuals.

3.9.2 Security Types

State the type(s) of security required and sepcify the need for the following as appropriate:

- Control Access to the facility hosting the system
- Control Access by User Class. For example, "No user may access any part of this application who does not have at least a (specified) clearance."
- Control Access by Group Attribute. For example, one group of users may view an attribute but may not update, while another group may view AND update.
- Control Access by System Function. For example, "This function is available only to a System Administrator."
- The need for accreditation of the security measures adopted for the system. For example, “X-LEVEL protection must be certified by an independent authorized organization.”

3.10 System Availability

System availability is the time when the system must be available for use.

Specify the hours (including time zone) during which the system will be available to users. For example, "The system must be available to users Monday through Friday between the hours of 6:30 a.m. and 5:30 p.m. EST." If the system is supposed to be available in more than one time zone, specify the earliest start time and the latest stop time. Also include the times when usage is expected to be at its peak. These are times when the system unavailability is least acceptable.

Test Plan *(PT)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	

TEST PLAN

EXECUTIVE SUMMARY

The FAS' verification and validation (V&V) plan defines a Test as:

> *The FAS' verification and validation (V&V) plan defines a TEST as:*
>
> *"... the act of using real or simulated inputs to show that a product satisfies its requirements and, if it does not, to identify the specific differences between the expected and actual results."*

A test plan (TP) document, as a multiple-tests repository, describes the objectives, scope, approach and focus of a testing effort.

The process of preparing a TP document is a useful way to formulate the efforts needed to validate the acceptability of a product. The completed document will help people outside the test group to understand the 'why's and 'how's of validation.

In short, an organization develops a TP to simply ascertain that: "The product was built correctly".

1.0 OVERVIEW

1.1 Purpose

Tests are done at the end of each phase of the development process to ensure that the requirements are complete and testable and that design, code, documentation and data satisfy those requirements.

Describe the overall goals and objectives of the test processes, and why this TP document was created.

1.2 Background

Provide a description of history and other background leading up to the development process. Identify the user organizations and the location where the testing will be performed. Describe any prior testing, and note results that may affect this testing.

1.3 Scope

Present the testing scope. Note the:

- Functionality/Features/Behavior that are tested
- Functionality/Features/Behavior that are not tested.

1.4 Limitations and Constraints

Detail any business, product line or technical constraints that may have potential impact on the manner in which the test are to be conducted. Also, identify limitations imposed on the testing, whether they are due to lack of specialized test equipment, or of time or resources. Indicate what steps, if any, are being taken to reduce program risk because of the test limitations(s).

1.5 Glossary

Provide definitions for terms and acronyms used in the TP document.

2.0 TESTING

Detail the overall testing strategy and the logistics required to properly execute the TP tests.

2.1 Subjects

Identify the test subjects (components, modules, etc..) by name. Note the exclusions explicitly.

2.2 Strategy

Present the overall testing strategy. This should include the test levels: unit, integration, system security, user acceptance tests and the planning that is needed. The test environment must be also described in terms of milestones, schedules and the resources needed for the testing. Identify the responsibility for setting up the test environment, developing test data to be used during the test (if necessary), developing and performing the tests.

2.2.1 Unit Testing

Describe the strategy for unit testing. This includes an indication of the components that will undergo unit tests or the criteria to be used to select components for unit test.

2.2.2 Integration Testing

Specify the integration testing (also known as System Testing) strategy. Describe the test environment (which would normally consist of the target hardware using simulated operational data files and prepared test data.) Include a discussion of the order of integration: compliance with standards, satisfaction of functional and technical requirements, performance, response time, ability to operate under stressed conditions and the external system interfaces. Also, the system documents and training manuals are examined for accuracy, validity, completeness and usability.

2.2.3 Acceptance Testing

Present the strategy for integration testing. Describe the tests performed in a non-production environment that mirrors the system's eventual production environment. Every system feature is tested for correctness and satisfaction of functional requirements. Interoperability, reliability, all support documentations and the level to which the system meets the user requirements are evaluated. Performance tests will be executed to ensure that response time, run time, operator intervention requirements and reconciliation issues are addressed.

2.2.4 Regression Testing

Present the strategy for regression testing. Regression testing is the selective retesting of a software system that has been modified to ensure that:

- Problems (bugs) have been fixed and that no other previously working functions have failed as a result of such reparations;
- The newly added features have not created problems with the previous versions of the software.

Regression testing is initiated after a programmer has attempted to fix a recognized problem or has added source code to a program that may have inadvertently introduced errors. It is a quality control measure to ensure that the newly modified code still complies with its specified requirements and that unmodified code has not been affected by the maintenance activity.

2.3 Resources

Define the testing resources and staffing requirements, along with their roles and responsibilities.

2.4 Results

Specify the mechanisms for storing and evaluating the test results.

2.6 Metrics

Describe all test metrics to be used during the testing activity. The RVTM from FRD is a good example for this.

2.7 Tools and Environment

Discuss the test environment including tools, simulators, hardware, test files and other resources.

2.8 Test Schedule

Present a detailed schedule for any/all applicable levels of testing.

2.9 Reporting

Describe how the test results are reported. Include information on the report's scope, who prepares it, who reviews it, who approves it, and when it is to be submitted. This is usually in the form of a Test Analysis Report (RT) format.

3.0 PROCEDURES

Detail the test procedures including tactics, test level(s) and test cases.

3.1 Test Subject(s)

Identify the test to be performed for the named module, [sub]system and address the criteria discussed in the subsequent sections for each test.

3.2 Test Description

For each applicable test level, list the following information.

- Personnel
- Roles and responsibilities
- Schedules
- Budgets
- Logistics (i.e., support tools needed: automated & other)
- Preparation Activities (i.e., environment setup)
- Techniques and Tools (RVTM-based test cases, evaluation methods & criteria, etc)

Interface Control Document *(ICD)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	

INTERFACE CONTROL DOCUMENT

EXECUTIVE SUMMARY

An interface control document (ICD) describes the relationship between two components of a system in terms of data items and messages passed, protocols observed and timing and sequencing of events. It can describe the interaction between two software components, a software component and a hardware device or a user and a system. The ICD is also used where complex interfaces exist between software components that are being developed by different teams.

An ICD should only describe the interface itself, and not the characteristics of the systems which use it to connect. The function and logic of those systems should be described in their own design documents if required. In this way, independent teams can develop the connecting systems which use the interface specified, without regard to how other systems will react to data and signals which are sent over the interface. For example, the ICD must include information about the size and format of the data, but not the meaning of the data and how the recipient should react to it.

A well defined ICD will allow one team to test its interface implementation by simulating the opposing side with simple communications simulators. Not knowing the business logic of the system on the other side of the interface, makes it more likely that one will develop a system that does not break when the other side changes its rules and logic. Thus, good modularity and abstraction leading to easy maintenance and extensibility are achieved.

1.0 OVERVIEW

1.1 Purpose

Describe why this ICD was created and what it does accomplish. The following can be used as an example:

This ICD provides an outline for use in the specification of requirements imposed on one or more software configuration items (SCIs), hardware configuration items (HCIs), manual operations or other [sub]system components to achieve one or more interfaces among them.

1.2 Scope

Describe the scope of the ICD. The following wording can be used as an example:

This ICD specifies the interface(s) between:

- System1
- System2
- ....
- System N.

Overall, an ICD can cover requirements for any numbers or kinds of interfaces as applicable.

1.3 System Identification

Identify the interface participant systems, the development contractors, the interfacing entities and the interfaces to which this ICD applies, including identification numbers(s), title(s), abbreviation(s), version number(s), release number(s) or any lower level version descriptors. A separate paragraph should be dedicated to each interface participant system.

1.3.1 System 1

Provide detailed information about interface participant System 1, the contractors developing/maintaining the systems, and the manager in-charge of interface.

1.3.2 System 2

The same relevant information must be provided for interface participant System 2.

1.4 Reference Documents

List the number, title, revision, date of all documents referenced or used in the preparation of this ICD. Including standards, governance or any other sort of applicable documents (Government or otherwise.)

2.0 DESCRIPTION

Provide a description of the interface between System 1 and System 2.

2.1 System Overview

For each interfacing system, summarize the functionality related to the interface, along with hardware and software components and the functions, data exchanges, transactions and security requirements.

2.2 Functional Allocation

Detail each interfacing system's functionality and the end users' involvements in the interface (during and after.) If the end users do not interact directly with the subject interface, describe the events that trigger the movement of information during the interface.

2.3 Data Transfer

Describe how data will be exchanged via the proposed interface. Include descriptions and diagrams of how connectivity among the systems will be implemented and of the type of messaging or packaging of data that will be transferred.

2.4 Transactions

Discuss transactions types that will be used to move data among the proposed interface components.

2.5 Security and Integrity

If the proposed interface has security and integrity requirements, detail how they will be addressed and how the data transmission security will be handled. Include details for the following:

- The transmission medium and whether it is a public or a secure line;
- The data protection during transmission and if/how data integrity is guaranteed;
- The guarantee that the interfacing systems will indeed interface with each other as intended and not with a rogue system masquerading as one of them;
- The mechanism for holding an individual on one system accountable for the resulting actions on the other component of the interface.

3.0 REQUIREMENTS

As mentioned earlier, an ICD can describe the interaction between a software component and a piece of hardware, a user and a system, and software components being developed by different sources. Each of these types of interfaces, have their own specific set of requirements. This ICD template provides a generic approach to interface requirements definition. FOR EACH INTERFACE ,THE FOLLOWING MUST BE PROVIDED:

3.1 Interface Requirements

*****The following is an example for the entire 3.1 section*****

This ICD specifies the interface requirement in regards with the following:

- Communication Methods – can be electronic networks or magnetic media;
- Data Protocol – may include messages and custom ASCII files;
- Processing Priority – indicate if the information is required to be formatted and communicated as a batch of data created by an operator or in accordance with some specifications and schedule; and
- Security – may include safety/security/privacy considerations.

3.1.1 Communication Methods

Describe the communication methods' requirements for presentation, session, network and data layers of the communication stack to which all interface participating systems must conform.

3.1.1.1 Initiation

Define the sequence of events by which the connections among the interface participating systems will be initiated. Include the minimum/maximum number of conceptions that will be supported. Also include the interface availability requirements (e.g., 24 hours a day, 7 days a week). Availability requirements beyond the control of the interfacing systems, such as network availability, are beyond the scope of an ICD.

3.1.1.2 Flow Control

Specify sequence numbering, legality checks, error control and recovery procedures that will be used to manage the interface. Include any acknowledgment (ACK/NAK) messages related to these procedures.

3.1.2 Data Protocol

Explicitly define the conditions under which a message is to be sent. The definition, characteristics and attributes of the command should be thoroughly described.

3.1.2.1 Assembly Characteristics

Present the message contents and formats, file or other data elements assembly (records, arrays, displays, reports, etc.) In defining the interfaces where data is moved among systems, define the packaging of data. When a relevant packaging technique is used, the following information should be provided:

- Names/identifiers/Abbreviations or synonymous names
- Project-unique identifier
- Non-technical (natural language) and Technical name (e.g., record or data structure name in code or database)
- Structure of data element assembly
- Visual characteristics of displays/outputs (layouts, fonts, icons and other display elements, beeps, lights) where relevant
- Relationships among different types of data element assemblies used for the interface
- Priority, timing, frequency, volume, sequencing, and other constraints and business rules
- Sources (setting/sending entities) and recipients (using/receiving entities)

3.1.2.2 Field/Element Definition

Define the characteristics of individual data elements defined above (see section 3.1.2.1) to include only features relevant to the interface being defined:

- Names/identifiers/Abbreviations or synonymous names
- Project-unique identifier
- Non-technical (natural language) and Technical name (e.g., record or data structure name in code or database)
- Priority, timing, frequency, volume, sequencing, and other constraints and business rules
- GSA/FAS standard data element name
- Data type (alphanumeric, integer, etc.)
- Size and format (such as length and punctuation of a character string)
- Units of measurement (such as meters, dollars, nanoseconds)
- Range or enumeration of possible values (such as 0-99)
- Accuracy (how correct) and precision (number of significant digits)
- Security and privacy constraints
- Sources (setting/sending entitles) and recipients (using/receiving entities)

3.1.3 Processing Priority

State the interfacing entities' performance and/or response time requirements that define how fast the incoming traffic or data requests must be processed. Latitude should be given in defining performance requirements to account for differences in hardware and transaction volumes at different interface sites. The response time requirements, which are impacted by resources and beyond the control of the interfacing systems (i.e., communication networks), are beyond the scope of an ICD.

3.1.4 Security Requirements

Discuss the security features that are required to be implemented within the message or file structure or the communications methods (safety/security/privacy considerations, encryption, authentication, compartmentalization, and auditing). Do not specify the requirements for features not provided by the systems to which the ICD applies. If the interface relies solely on physical security or on the network's security and the firewalls through which the systems are connected, so state.

4.0 EVALUATION

Normally, an evaluation/qualification campaign can be achieved by one (or all) of the following efforts:

- Analysis of accumulated data obtained from other evaluations. Examples are reduction, interpretation or extrapolation of test results;
- Demonstration means the operation of interfacing entities that relies on observable functional operation not requiring the use of instrumentation, special test equipment, or subsequent analysis;
- Inspection consists of the visual examination of interfacing entities, documentation, etc;
- Special Qualification – Any special qualification methods for the interfacing entities, such as special tools, techniques, procedures, facilities, and acceptance limits; and
- Testing which is the operation of interfacing entities using instrumentation or special test equipment to collect data for later analysis.

Detail how the results of the interface will be evaluated and who will be responsible for the evaluation.

5.0 NOTES

Compile and present all applicable notes relevant to the interface campaign.

Conversion Plan

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	

CONVERSION PLAN

EXECUTIVE SUMMARY

A Conversion Plan (CP) document describes how to convert data from an existing system to another hardware or software environment. It provides installation and conversion procedures a site and is used to discuss conversion procedures for installation; co-ordination procedure; installation procedures for new/converted files and/or databases.

1.0 INTRODUCTION

This CP provides installation and conversion procedures for [replacewithapplicable]. It is prepared at the start of the begin phase and finalized with additional detail at the evaluate stage.

1.1 Purpose

Present the purpose of the conversion plan as:

- Conversion procedures for the installation;
- Coordination procedures for the development of data conversion efforts; and
- Implementation procedures for the new/converted files and/or databases.

Also elaborate that, based on the factors to be considered for each system/project, the CP should:

- Determine if any portion of the conversion process should be performed manually;
- Determine if any parallel runs of the old and new systems are necessary during the conversion;
- Clarify data function in the old, and determine the usage of data in the new, system;
- Consider the order that the data is processed in the two systems;
- Consider volumes, such as the database size and the amount of data to be converted;
- User work and delivery schedules and time frames for reports, etc;
- Determine if the data availability and use should be limited during the conversion process; and
- Determine the disposition of obsolete or unused data that is not converted.

1.2 Scope

Describe the boundaries of the conversion effort for the following:

- Functions and/or data not affected or converted;
- Conversion Processes and Procedures;
- Phased/Staged Implementation Procedures; and
- Functions affected by the conversion process.

1.3 Project References

Provide a list of the references that were used in preparation of this CP document.

1.4 Glossary

Insert a list containing a glossary of all terms and abbreviations used in the plan.

2.0 CONVERSION DETAILS

Describe the detailed activities, resources and schedule associated with the conversion.

2.1 System Overview

Provide an overview of the system undergoing conversion. If it is a database or an information system, also include a general discussion of the type of data maintained, the operational sources and the uses of those data.

2.2 Requirements

If the conversion is planned to be executed in discrete phases, identify what components will undergo conversion in what phase (hardware, software and data as appropriate.) Develop and continuously update a milestone chart for the conversion process. If only selected system parts will be targeted for conversion, identify which components will and will not be converted.

Continue by identifying and addressing the following:

- Input data that is to be converted (prior to its new usage). This should include its name, source form or record layout, storage medium, location, volume, size, access method and security concerns;
- Specifications on how the conversion will be done. If computer programs are to be used, give their specifications (i.e., program logic, interfaces, error/exception processes, etc.);
- Output data which will result from the conversion process. This should include its name, record layout, storage medium, location, volume, size, access method and security considerations; and Validation tools to include a detailed description of the manual and/or automated controls and methods to be used to ensure that all data intended for conversion have been converted.

2.3 Strategy

Describe, if applicable, the strategies for the conversion of:

- Data – Include the specific input data requirements and its preparation for the conversion. If the data will be transported from the original system, provide a detailed description of data handling, conversion and loading procedures. If the data will be transported via machine-readable media, describe the media characteristics. Also discuss the data conversion strategy and controls, as well as the required quality assurance efforts.
- Hardware – In case of a hardware platform conversion --i.e., mainframe to client/server-- the interfaces to other systems may need reengineering. Elaborate the affected interfaces and the revisions required in each.
- Software – Present the strategy for ensuring data quality pre/post-conversion. Also, describe the approach to data scrubbing and quality assessment of data before they are moved to the new or converted system. The strategy and approach may be described in a formal transition plan or a separate document if more appropriate.

2.4 Risk Factors

Identify conversion risk factors and strategies for their control and/or reduction. Include the descriptions of these factors that could affect the conversion feasibility, the technical performance of the converted system, the conversion schedule or costs. Additionally, a review should be made to ensure that the current backup and recovery procedures are operational and adequate.

2.5 Planning

Describe the planning for the conversion effort. If planning and related issues have been addressed in other life-cycle documents, reference those documents here.

The following can be used as an example for the conversion planning issues that you may want to address:

- Analysis of projected workload for the target environment to ensure that the projected environment can adequately handle that workload and meet performance and capacity requirements;
- Projection of the growth rate for the data processing needs in the target environment to ensure that the system can handle the projected near-term growth, and the expansion capacity for future, needs;
- Analysis to identify missing features in the target environment that were supported in the original environment; and
- Development of a strategy for recoding, reprogramming or redesigning the components of the system that used hardware and software features not supported in the target, but used in the original, environment.

2.6 Pre-Conversion Tasks

Identify the tasks that are logically separate from the conversion effort itself but that must be completed before the initiation, development or completion of the conversion effort.

The following can be used as an example for the Pre-Conversion effort tasks:

- Finalize decisions regarding the type of conversion to be pursued;
- Install changes to the system hardware, such as a new computer or communications hardware, if necessary;

- Implement changes to the computer operating system or its components, such as the installation of a new LAN operating system or a new windowing system;
- Acquire and install other software for the target environment, such a new DBMS or document imaging system.

2.7 Major Tasks & Procedures

Detail the major tasks associated with the conversion and the procedures associated with those tasks:

- Task Name – Provide the name and description for each major task required for the conversion, including preparation of data and testing of the system. If some of these tasks are described in other life-cycle documents, reference them here.
- Procedures – Describe the procedural approach by providing as much detail as necessary.

2.8 Schedule

Present the schedule for the conversion activities to depict the beginning and end dates of each task. Charts may be used as appropriate. DO NOT repeat the Pre-Conversion Tasks here.

2.9 Security

If applicable, provide an overview of the system security information as follows:

- The System Security Features' description should contain an overview and discussion of the Post-Conversion security features. Reference other documents as appropriate. Discuss changes in the security features or performance of the system that would result from the conversion.
- Security During Conversion should address security issues specifically related to the conversion.

3.0 CONVERSION SUPPORT

This section describes the support necessary to implement the system. If there are additional support requirements not covered by the categories shown here, add other subsections as needed.

3.1 Facilities

Identify the physical facilities and accommodations required during the conversion period.

3.2 Hardware

List the required support equipment, including all hardware to be used for the conversion.

3.3 Materials

List the support materials.

3.4 Personnel

If applicable, discuss the personnel requirements as follows:

- Personnel Requirements & Staffing – Describes the number of personnel, length of time needed, types of skills and skill levels for the staff required for the conversion;
- Training of Conversion Staff – Address the staff training (if any) needed for the conversion. Present a training curriculum which lists the courses to be provided, a course sequence and a proposed schedule. If appropriate, identify (by job description) which courses should be attended by particular types of staff. Training for users in the system operation is not presented here, but is normally included in the Training Plan.

3.5 Software

Identify the software and databases needed to support the conversion. Describe all software tools used to support the conversion effort, including the following types of software tools, if used:

- Automated conversion, like translation tools, for translating among different computer languages or software families (i.e., between release versions of compilers and DBMSs);
- Automated data conversion tools for translating among storage formats associated with different implementations (i.e., different DBMSs or operating systems);

- Automated testing and quality assurance and validation software for the data conversion;
- Computer-aided software engineering (CASE) tools for reverse engineering;
- CASE tools for capturing system design information and presenting it graphically;
- Documentation tools such as cross-reference lists and data attribute generators;
- Commercial off-the-shelf software and software written specifically for the conversion effort

System Design Document *(SDD)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

SYSTEM DESIGN DOCUMENT

EXECUTIVE SUMMARY

The system design document (SDD) is the logical successor to the functional requirements document (FRD) and describes how to transform the requirements embedded in FRD into technical system design specifications that will eventually be used for developing a new system (or modifying an existing one.)

SDD is primarily used by: the project manager, the development manager, the IT manager, the technical architect and the systems administrator.

1.0 INTRODUCTION

1.1 Purpose

This SDD is used to translate the previously recorded system requirements and objectives (see section 1.4, below) into technical system design specifications.

1.2 Project Summary

Describe the project from a management perspective and provide an overview of the framework within which the conceptual system design was prepared. If appropriate, include the information discussed in the subsequent manner:

- System Overview – Describe the system narratively and in non-technical terms. Include a high-level system architecture diagram showing a subsystem breakout of the system, if applicable. The high-level system architecture or subsystem diagrams should show interfaces to external systems. Supply a high-level context diagram for the system and/or subsystems, if applicable. Refer to the FRD’s requirements verification traceability matrix (RVTM) to identify the allocation of the functional requirements into the SDD;
- Design Constraints – Present possible system design constraints (reference any trade-off analyses conducted) and include any assumptions made by the project team in developing the SDD;
- Future Contingencies – Discuss any contingencies that might arise in the design of the system that may change the development direction. Possibilities include lack of interface agreements with outside agencies or unstable architectures at the time this document is produced. Address any possible workarounds or alternative plans.

1.3 Document Organization

This section describes the organization of the SDD.

1.4 Project References

Provide a bibliography of key project references and work products that have been produced prior to this point. For example, these references might include the Project Management Plan, Feasibility Study, CBA, Acquisition Plan, QA Plan, CM Plan, FRD and ICD.

1.5 Glossary

Supply a glossary of all terms and abbreviations used in this document. If the glossary is several pages in length, it may be included as an appendix.

2.0 ARCHITECTURE

Here, describe the project’s system and/or subsystem(s) architecture. Support your descriptions by graphics and schematics where appropriate. References to external entities should be minimal, as they will be described later on in the SDD.

2.1 Hardware

Detail the system hardware and organization including a list of components and diagrams showing the connectivity between the components. If appropriate, use subsections to address each subsystem.

2.2 Internal Communications

Describe the system's internal communications (LANs, buses, etc.) Include architectures (X.25, Ethernet, etc.) Provide a diagram* showing the communications path(s) between system and subsystem modules. If appropriate, use subsections to address each architecture being employed.

*The diagrams should map to the FRD context diagrams.

2.3 Software

Present the system's software and organization. Include a list of software modules (functions, subroutines, or classes), computer languages and programming computer-aided software engineering tools. Use the structured organization diagrams/object-oriented diagrams that show various segmentation levels down to the lowest level. All features on the diagrams* should have reference numbers and names. Include a narrative that expands on and enhances the understanding of the functional breakdown. If appropriate, use subsections to address each module.

*The diagrams should map to the FRD data flow diagrams, providing the physical process and data flow related to the FRD logical process and data flow.

3.0 FILE AND DATABASE DESIGN

You may need to collaborate with your resident database administrator (DBA) in preparing this section. Here, reveal the final design of database management system (DBMS) and Non-DBMS files associated with your system. Additional information may be added as required for the particular project. Provide a data dictionary showing data element name, type, length, source, validation rules, maintenance (create, read, update, delete – CRUD-- capability), data stores, outputs, aliases and description.

3.1 DBMS Files

Present the final design of the DBMS files to include the following information:

- Refined logical model; provide normalized table layouts, entity relationship diagrams and other logical design information;
- Physical description of the [sub]schemas, records, sets, tables, storage page sizes, etc.;
- Access methods (i.e., indexed, via set, sequential, random access, sorted pointer array, etc.);
- Estimate of the file size or volume of data within the file, data pages and the overhead resulting from access methods and free space;
- Definition of update frequency of the database tables, views, files, areas, records, sets and data pages; estimate the number of transactions if the database is online transaction-based.

3.2 Non-DBMS Files

Provide the detailed description of all non-DBMS files to include a narrative description of the usage for each file (i.e., input, output, or both; temporary file; the modules that read and write the file, etc.) and the file structures (from the data dictionary). If possible, the file structure information should:

- Identify record structures, keys or indices and reference data elements within the records;
- Define record length (fixed or maximum variable length) and blocking factors;
- Define file access method (ISAM, Random, virtual sequential, etc.);
- Estimate the size or data volume within the file, and the overhead from the access methods;
- Define the file update frequency. If the file is part of an online transaction-based system, provide an estimated number of transactions per unit time, the statistical mean, mode and distribution of those transactions.

4.0 DETAILED DESIGN

This section provides the information needed for the development team to actually build and integrate the hardware components, code and integrate software modules and interconnect the hardware and software segments into a system product. Additionally, this section details the procedures for combining separate commercial off-the-shelf (COTS) packages into a single system. Every detailed requirement should map back to the FRD, and the mapping should be presented as an update to the RVTM.

4.1 Hardware

A hardware component is the lowest level of the system design's granularity. Depending on the design requirements, there may be one or more components per system. This section should provide enough detailed information about individual component requirements to correctly build and/or procure all the system hardware (or integrate COTS items). Add additional diagrams and information to describe each component and its functions adequately. Industry-standard component specification practices should be followed. Include the following –representative sample-- information as applicable:

- Power input requirements for each component
- Signal impedances and logic states
- Connector specifications (serial/parallel, 11-pin, male/female, etc.)
- Memory and/or storage space requirements
- Processor requirements (speed and functionality)
- Graphical representation depicting the number of hardware items (i.e., monitors, printers, servers, I/O devices), and the relative positioning of the components to each other
- Cable type(s) and length(s)
- User interfaces (buttons, toggle switches, etc.)
- Hard drive/floppy drive/CD-ROM requirements
- Monitor resolution

For COTS procurements, if a specific vendor has been identified, include appropriate item information.

4.2 Software

Provide the detailed design of the system and subsystem relative to input, processes and output. Any additional information may be added to this section and organized according to whatever structure best presents the design continuum. Depending on the particular nature of the project, it may be appropriate to repeat these sections at both the subsystem and design module levels. Additional information may be added to the subsections if the suggested lists are inadequate to describe the system design.

4.2.1 Inputs

Discuss the input media used by the operator for providing information to the system; show a mapping to the high-level data flows described in the System Overview part of paragraph 1.2 (i.e., data entry screens, optical character readers, bar scanners, etc.) If appropriate, the input record types, file structures and database structures provided in paragraph 3.0 may be referenced.

In addition, provide the layout of all input data screens or graphical user interfaces (GUIs) and a graphic representation of each interface. Also define all data elements associated with each screen or GUI, or reference the data dictionary.

Finally, make sure to include the following –representative sample-- information in this section:

- Data elements' edit criteria (i.e., specific values/range, mandatory/optional, alphanumeric values and length);
- Data entry controls to prevent edit bypassing; and
- Miscellaneous messages associated with operator inputs, including the:
  - Copies of form(s) if the input data are keyed or scanned for data entry from printed forms
  - Description of any access restrictions or security considerations
  - Each transaction name, code, and definition, if the system is a transaction-based processing system
  - Incorporation of the Privacy Act statement into the screen flow, if the system is covered by the Privacy Act.

4.2.2 Processes

Processes constitute the lowest level of design granularity in any system. Depending on the software development approach, there may be one or multiple modules per system. Here, you should provide enough detailed information about the logic and data necessary to completely write source code for all modules in the system (and/or specific user-exits to integrate COTS software programs).

Insert diagrams and information to describe each module, its functionality and hierarchy (if necessary). Include the following –representative sample-- information for every detailed module design:

- A narrative description, function, conditions under which it is used (called or scheduled for execution), processing logic, interfaces to other modules, external interfaces, security requirements, detail of any algorithms used by the module;
- For COTS packages, specify any call routines or bridging programs to integrate the package with the system and/or other COTS packages (i.e., DLLs);
- Data elements, record structures and file structures associated with module's input and output;
- Graphical representation of the module processing logic, flow of control, and algorithms, using an accepted diagramming approach (i.e., structure charts, action diagrams, flowcharts, etc.);
- Data entry and data output graphics; define or reference associated data elements (if the project is large and complex or if the detailed module designs will be incorporated into a separate document, then it may be appropriate to repeat the screen information in this section).

4.2.3 Outputs

Show a mapping to the high-level data flows in the System Overview part of paragraph 1.2. Reference the output files described in paragraph 3.0 and provide the following –representative sample-- information:

- Description of report, and screen, codes, names, layouts and contents;
- Description of the purpose of the output, including identification of the primary users Report distribution requirements, if any (include frequency for periodic reports);
- Description of any access restrictions or security considerations.

5.0 INTERFACES*

Generally speaking, interfaces come in two different forms:

- Internal Interface which is defined as a connection to the LAN side of a router, and is in contrast with
- External Interface which is a connection to the WAN side of a router (can be a public or private network.)

When designing interfaces, special attention must be paid to the specific natures and requirements of the above-mentioned interface methods.

In this section, describe the interface(s) between the system being developed and other systems; for example, batch transfers, queries, etc. Include the interface architecture(s) being implemented, such as wide area networks, gateways, etc. Provide a diagram depicting the communications path(s) between this system and each of the other systems, which should map to the context diagrams in Section 1.2.1. If appropriate, use subsections to address each interface being implemented.

*If a formal ICD exists for a given interface, the information can be copied, or the ICD can be referenced in this section.

5.1 Internal

If a system consists of more than one component, there may be a requirement for internal interfaces to exchange information, provide commands or support input/output functions. This section should provide enough detailed information about the communications requirements to correctly build and/or procure interface components for the system. Include the following –representative sample-- information:

- The LAN topology;
- The number of servers and clients to be included on each LAN;
- Specifications for bus timing requirements and bus control;
- Format(s) for data being exchanged between components; and........
- Graphical representation of the connectivity between components showing the direction of data flow and approximate distances between components; information should provide enough detail to support the procurement of hardware to complete the installation at a given location.

5.2 External

Describe the electronic interface(s) between this system and other systems from the point of view of the system being developed.

For every interface participating system, provide the information exchange and interface rules. Detail the requirements for correct formatting, transmission and/or reception of data, including the following:

- Data Format Requirements. If there is a need to reformat data before they are transmitted or after the incoming data is received, tools and/or methods for the reformat process should be defined;
- Hand-Shaking Specifications. Such protocols between the systems must be identified. Include the content and format of the information for the hand-shake messages, the timing for exchanging these messages and the steps to be taken when errors are encountered;
- Error Handling & Reports. Must specify formats of error reports exchanged between the systems and their disposition (i.e., retained in a file, sent to a printer, flag/alarm sent to the operator, etc.);
- Graphical Representation of the connectivity between systems showing the direction of data flow;
- Query & Response Specifications.

6.0 SECURITY CONTROLS

The developers of GSA FAS' systems are required to adhere to different security control levels. Discuss the security controls required to be implemented within the message, file structure or communications methods (safety/security/privacy considerations, encryption, authentication, compartmentalization, and auditing). At the minimum, provide the following –representative sample-- information:

- Mechanisms to assign role-based and/or restricted access to critical data;
- Audit procedures to meet control, reporting and retention period requirements for operational and management reports;
- Application audit trails to dynamically audit retrieval access to designated critical data;
- Standard Tables to be used or requested for validating data fields;
- Verification processes for additions, deletions or updates of critical data; and.......
- Ability to identify all audit information by user identification, network terminal identification, date, time, and data accessed or changed.

Implementation Plan *(IMP)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

IMPLEMENTATION PLAN

EXECUTIVE SUMMARY

A key difference between system implementation and all other phases of the lifecycle is that all project activities up to this point have been performed in safe, protected and secure environments, where project issues that arise have little or no impact on day-to-day business operations. Once the system goes live, however, that would no longer be the case. Any miscues at that point will certainly translate into direct operational and/or financial impacts on the performing organization. It is through the careful planning, execution and management of the system implementation activities that the project team can minimize the likelihood of these problematic occurrences and determine appropriate contingency plans.

1.0 INTRODUCTION

The system implementation plan (IP) document describes how an information system will be deployed, installed and transitioned into a new operational environment. It contains an overview of the system, a brief description of the major tasks involved in the implementation, the resources needed to support the implementation effort (hardware, software, facilities, materials and personnel), and site-specific implementation requirements.

The IP is developed during the design phase; updated during the development phase; and provided in its final form during the integration and testing , as well as the implementation, phases.

1.1 Purpose

The purpose of IP, then, can be summarized as follows:

- Deployment – Making the new system available to a prepared set of users; and
- Transition – Positioning the system's support and maintenance within the performing organization.

At a finer detail level, deploying a system consists of executing all steps necessary to educate the users on the use of the new system, placing the newly developed system into production, confirming that all data required at the start of operations is available and accurate and validating that business functions that interact with the system are functioning properly. Transitioning the system support responsibilities involves changing from development to support and maintenance mode of operation, with ownership of the new system moving from the project team to the performing organization.

1.2 System Overview

Provide, from a management' perspective, an overview of the to-be-implemented system, its description and organization:

- Description – Describe the processes that the system is intended to support. If it is a database or an information system, provide a general discussion of the description of the type of data maintained and the operational sources and uses of those data;

- Organization – Present a description of system structure and the major components essential for it implementation including both hardware and software. Charts, diagrams and graphics may be included as necessary.

1.3 Project References

Provide a bibliography of key project references and work products that have been produced prior to this point. For example, these references might include the Project Management Plan, Acquisition Plan, FRD, Test Plan, Conversion Plan and SDD.

1.4 Glossary

Supply a glossary of all terms and abbreviations used in this document. If the glossary is several pages in length, it may be included as an appendix.

2.0 IMPLEMENTATION DETAILS

Drill down the implementation process from a management perspective and provide an overview of the framework within which the IP document was prepared. Make sure to clarify that in any given successful implementation campaign, emphasis is to be placed on both, the processes and the people responsible for carrying them out (see below.)

2.1 The Team

Identify system proponent, the name of responsible organization(s), and titles and telephone numbers of the following staff (sorted alphabetically) who serve as points of contact for the system implementation:

- Application Developers
- Business Analysts
- Configuration Manager
- Database Administrator
- Data/Process Modeler
- Information Security Officer (ISO)
- Other Stakeholders (or their representatives)
- Project Manager
- Project Sponsor
- Quality Assurance (QA) Manager
- Site Implementation Representative(s)
- Technical Lead/Architects
- Technical Services (HW/SW, LAN/WAN, TelCom)
- Technical Support
- User Community Decision-Maker(s)
- User Representative(s)
- Users

2.2 The Effort

Detail the implementation phase activities to consist of the following processes:

- Prepare for implementation, where all steps needed in advance of actual application deployment are performed, including preparation of both the production environment and user communities;
- Deploy the system, where the full deployment plan, initially developed during the design phase and evolved throughout subsequent lifecycle phases, is executed and validated; and ....
- Transition the system, where responsibility for and ownership of the application are transitioned from project team to the unit in performing organization that will provide support and maintenance.

3.0 PREPARATION

In implementing a new system, it is necessary to ensure that the user community is best positioned to use the system once its deployment is validated. Therefore, all necessary training activities should be scheduled and coordinated. As this training is often the first system exposure for many individuals, it should be conducted as professionally and competently as possible. A positive training experience is a great first step towards the user acceptance of the system.

Also, more than at any point in the project, the project manager must plan for failure and must have a defined set of contingency plans to be executed if/when problems are encountered problems during the implementation. The stakeholders must clearly understand and agree to the various Go/No-Go decision making criteria.

Using a mechanism similar to the table below, document all major tasks required for the implementation. The tasks described in this –sample table– are not site-specific, but totally generic in nature and represent a series of project tasks required for installing hardware and software, preparing data and verifying the results. Include the following –representative sample-- information as appropriate:

Task Name	Required Resources	Responsible Person	Measurement of Success
Acquire special hardware or software			

Ensure that all prerequisites have been fulfilled before the implementation date			
Ensure availability of support documentation			
Perform data conversion before loading			
Perform site surveys before implementation			
Prepare site facilities for implementation			
Provide appropriate training for personnel			
Provide personnel for the implementation team			
Provide planning and coordination for implementation			
Provide required technical assistance			
Schedule special computer processing required			
Develop implementation and transition plan document			

3.1 Schedule

Provide a schedule of activities to be accomplished during implementation. Show the major tasks (see paragraph 2.3, above) in chronological order, with the beginning and end dates for each task.

3.2 Security

If applicable, present the system security features and requirements during the implementation. If the system is covered by the Privacy Act, provide Privacy Act concerns.

3.2.1 Features

Provide a discussion of system security features after the implementation, including the primary security features for both hardware and software. Also, security and protection of sensitive data and information should be discussed, if applicable.

3.2.2 During Implementation

Address the anticipated specific security issues during the implementation effort (if any.) For example, if LAN servers or workstations will be installed at a site with sensitive data preloaded on non-removable hard disk drives, explain how security would be provided for the data on these devices during shipping, transport and installation.

4.0 DEPLOYMENT

Describe the support software, materials, equipment, and facilities required for the implementation, as well as the personnel requirements and training necessary for the implementation. The information provided in this section is not site-specific. If there are additional support requirements not covered by the subsequent sections, they must be added as needed.

4.1 Facilities, Hardware, Material and Software

4.1.1 Facilities

Identify the physical facilities and accommodations required during implementation. Include the physical workspace for assembling and testing hardware components, desk space for software installers and classroom space for training the implementation staff. Specify the hours per day needed, number of days and anticipated dates.

4.1.2 Hardware

Provide a list of all support equipment including all hardware used for testing the implementation.

4.1.3 Materials

List the required support materials, such as magnetic tapes and CDs.

4.1.4 Software

Detail the software and databases required to support the implementation by name, code or acronym. Identify the COTS, GSA-Specific and any software that is specifically used to facilitate the implementation process.

4.2 Personnel

Present the personnel requirements including any known or proposed skill-set requirements. Describe the training, if any, to be provided for the implementation staff.

4.2.1 Staffing Requirements

Identify the number of personnel, length of time needed and the skill type and levels required during the implementation. If a particular staff has been selected or proposed for the implementation, identify them and their roles in the implementation.

4.2.2 Staff Training Requirements

Detail the training necessary to prepare the staff for implementing and maintaining the new system. Do not include the user training here. List the type and length of the training needed for the following areas:

- Hardware and Software Installation;
- System Support (including Help Desk); and
- Maintenance and Enhancement.

5.0 TRANSITION & “BACK-OFF” PLAN

In many organizations, the team of individuals responsible for the long-term support and maintenance of a system is different from the team initially responsible for designing and developing the application. Often, the two teams include a comparable set of technical skills. The responsibilities associated with supporting an operational system, however, are different from those associated with new development.

To effect this shift of responsibilities, the project team must provide those responsible for system support in the performing organization with a combination of technical documentation, training and hands-on help to enable them to provide an acceptable level of operational support to the users. This transition is one element (albeit a major one) of the overall implementation and transition plan. The project manager should review the transition plan to confirm that all defined actions have been successfully completed.

As far as the measurements of success go, the implementation itself serves as its own measurement of success. In fact, a smooth implementation culminates --and validates-- the system development effort.

Nevertheless, even before the final turnover, the project manager should use the measurement criteria below to assess the implementation proceeding’s success. More than one “No” answer indicates a serious risk to the success of the step, and for that matter, the entire project.

Step	Measurement of Success	Yes	No
Prepare	• Has anyone verified that every user has the correct level of system access and security?	🟩	🟥

	- Is there a checklist of all system components that can be used to verify that all correct versions of all components of the system are in the new production environment?	🟩	🟥
	- Do the managers of technical services and technical support agree with your estimate of extra work for their units associated with the new system deployment?	🟩	🟥
Deploy	- Do your team members agree that their part of the effort as outlined in the implementation and transition plan is reasonable and achievable?	🟩	🟥
	- Do the training and evaluation forms filled out by the users and customers being trained in the new system reflect the scores equal to, or higher than, those anticipated the implementation and transition plan?	🟩	🟥
	- Have you had to "*freeze*" or "*fall-back*" in your development activities more than originally anticipated in the deployment plan?	🟩	🟥
	- Are volumes of support calls within the range originally anticipated in the deployment plan?	🟩	🟥
Transition	- Has the *performing organization* agreed to transition all of the remaining defects along with the new system itself?	🟩	🟥

If it was decided that the implementation was not a success, describe how the noted discrepancies will be rectified and present a detailed action item list.

In case of a No-Go decision, devise a very detailed “Back-Off” plan with instructions on how to restore the installation to its exact original, pre-conversion condition.

Maintenance Manual *(MM)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

EXECUTIVE SUMMARY

The Maintenance Manual (MM) document presents information on the system. It is written for personnel who are responsible for the maintenance of the system and who need to understand the operating environment, security, and control requirements. It describes the programs in technical detail to assist the maintenance programmer.

Supplementary information may be included in the MM to facilitate maintenance and modification of the system. Appendices to document various maintenance procedures, standards or any other essential information may be added to this document, when warranted.

1.0 INTRODUCTION

1.1 Purpose

The purpose of MM should be provided here (Similar text as the Executive Summary, above, can be used.)

1.2 System Overview

Provide an overview of the system as follows:

- Responsible Organization
- General Description
- Category, Code and Name/Title
- Environment or special conditions
- System Architecture --in non-technical terms-- (e.g., client/server, web-based, etc.)
- Major Functions
- User Access Mode (e.g., graphical user interface)
- Operational Status (D/M/E or O&M.)

1.3 Project References

Present a list of the references that were used in preparation of this MM document in order of importance to the end user.

1.4 Points of Contact

1.4.1 Information

Provide a list of the points of organizational contact (POCs) that may be needed by the document user for informational and troubleshooting purposes. Include the type of contact, contact name, department, telephone number and e-mail address.

1.4.2 Coordination

List the organizations that may require coordination between the project and its specific support function (e.g., installation coordination, security, etc.). Include a schedule for coordination activities.

1.5 Glossary

Supply a glossary of all terms and abbreviations used in this document. If the glossary is several pages in length, it may be included as an appendix.

2.0 SYSTEM DESCRIPTION

2.1 Architecture

Describe the [sub]system, communications, etc., in terms of their overall relationships. Accompany the description with a graphic representation depicting the interrelationships of the major components of the system. Show the systems communications network for networked or distributed processing support.

2.2 Security

Detail the security considerations associated with the system.

3.0 ENVIRONMENT

3.1 Equipment Environment

Describe the equipment configuration.

3.2 Storage Requirements

Describe the amount and types of storage required to operate the system, the broad parameters of the storage locations and resources that are required, and any algorithms used to determine that amount.

3.3 Support Software Environment

List the support or special purpose software used by the system including DBMS utility software and CM software. Identify the current version or release number under which the system is being maintained.

4.0 SYSTEM MAINTENANCE PROCEDURES

4.1 Responsibilities

Identify the responsible organization(s) and personnel, including telephone numbers and email addresses, for system maintenance.

4.2 Conventions

Explain rules and conventions that have been used within the system and database. Include such information as:

- Design of mnemonic identifiers and their application to the labeling of software units, sub-units, data structures, data elements, storage areas, etc. Describe provisions for unique naming or renaming at different sites if contingency processing at alternate sites requires separation of the resources named by the identifiers;
- Procedures and standards for graphic representations, listings, abbreviations used in statements and remarks, and symbols appearing in charts and listings;
- The appropriate standards, fully identified, may be referenced in lieu of a detailed outline of conventions;
- Standard data elements and related features.

4.3 Performance Verification Procedures

Identify the procedures necessary to verify the performance of the system.

4.4 Error Conditions

List all error messages produced by the system to include identification of the error, description of the error, an explanation of the source of the error and recommended methods to correct it.

4.5 Maintenance Procedures

This section provides a detailed description of system maintenance procedures, which may include utilities, verification methods, and other procedures necessary to maintain the system input-output components (such as the database) or to perform special maintenance runs. Each procedure should be under a separate section header, 4.5.1 - 4.5.x.

4.5.x [Maintenance Procedure Name]

Provide a maintenance procedure identifier for reference in the remainder of the subsection. Describe the maintenance procedure and the appropriate sequencing for its setting up, running, and terminatoin.

5.0 SOFTWARE UNIT MAINTENANCE PROCEDURES

5.1 Consolidated Unit List

Provide the consolidated software unit list.

*****Each software unit in the following sections should be under a separate section header, 5.2 - 5.x.*****

5.x [Software Unit Identifier]

Identify and describe the system software unit.

5.x.1 Description

Provide detailed characteristics of the software unit and its relationship to other software units.

5.x.2 Functions

List and describe the functions being performed by the software unit.

5.x.3 Input

Identify and describe the input, if applicable. Include the following information:

- Input data format (data record layout)
- Source and medium of each type of input

5.x.4 Processing

Provide detailed description for the following:

- Initiation Procedures – Such as software calls and parameters, and job control statements;
- Core Processing Procedures of the software unit. Include descriptions of input acceptance, accessing a database, decision points and output production;
- Branching Conditions – Major branching conditions provided in the software unit;
- Restrictions that have been designed into the system with respect to the operation of this software unit (such as any limitations on the use of the software unit and any timing requirements);
- Exit Requirements – The exit criteria for termination of the operation of the software unit;
- Communications or linkage to the next logical software unit;
- Output produced by the software unit for use by related software units;
- Unique Features for executing the software, such as diagnostic modes not documentd in any support documentations.

5.x.5 Data Structures

List data structures described in the next section, used within the software unit, if applicable. If the data description of the software unit provides sufficient information, the software listing may be referenced to provide some of the information. Include at a minimum, the following types of information:

- Structure name, label, or symbolic name
- Purpose
- Other software units that use this data structure
- Logical divisions within the data structure
- Data structure description access paths (these may be represented graphically)

5.x.6 Verification Procedures

Present the requirements and unique procedures necessary to verify the performance of the software unit.

5.x.7 Listings

Identify the software listing's locatione. Comments appropriate to particular instructions may be included to understand and follow the listing.

5.x.8 Interfaces

Describe the software unit interfaces with other software units.

6.0 DATABASE MAINTENANCE PROCEDURES

This section provides the information necessary to maintain the databases of the system. Each database maintenance procedure should be under a separate section header, 6.1 – 6.x.

6.x [Database Identifier]

Specify the database name and mnemonic ID. List the software units using the database. Include a complete description of the purpose and content of each database used by the system, including security considerations. Specify the database structure (e.g., relational, object-oriented, flat file).

6.x.1 General Characteristics

Provide the logical and physical schemas for the database (reference location). Then proceed with the following:

- Permanency – Document whether the database contains static data that the software unit can reference, but may not change, or dynamic data that may be changed or updated during system operation. Indicate whether the change is periodic or random, as a function of input data;
- Storage – Specify the media for the database and the amounts of storage required;
- Restrictions – Explain any limitations on the database usage by the software units in the system.

6.x.2 Organization and Detailed Description

This subsection identifies and defines the internal architecture of the database.

- Structures of the physical records. Identify structure parts, such as control segments (keys) and the body of the record (physical storage schema).
- Elements – Identify each element in the structure, and if necessary, explain its purpose. Include for each segment the following items:
  - Labels: Indicate the label assigned to reference each element.
  - Size: Indicate the length and number of characters/bits that make up each data element.
- Expansion – Document provisions, if any, for adding to the structure.
- Contingencies – Document provisions, if any, for extracting subsets of the database to permit operation in degraded modes or at alternate sites.
- Partitioning – Document where the database physically resides.

Operations Manual *(OM)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

OPERATIONS MANUAL

EXECUTIVE SUMMARY

The Operations Manual (OM) contains detailed information on the control requirements and operating procedures necessary to successfully initiate and run a system. It is written for the operations staff and who need to understand the operating environment, security and control requirements.

1.0 INTRODUCTION

1.1 Purpose

The purpose of OM should be provided here (Similar text as the Executive Summary, above, can be used.)

1.2 System Overview

Provide an overview of the system as follows:

- Responsible Organization
- General Description
- Category, Code and Name/Title
- Environment or special conditions
- System Architecture --in non-technical terms-- (e.g., client/server, web-based, etc.)
- Major Functions
- User Access Mode (e.g., graphical user interface)
- Operational Status (D/M/E or O&M.)

1.3 Project References

Provide a list of references that were used in preparation of this document in order of importance to the operations staff. This should, at a minimum, include the maintenance and users' manuals (MM and UM).

1.4 Points of Contact

1.4.1 Information

Provide a list of the points of organizational contact (POCs) that may be needed by the document user for informational and troubleshooting purposes. Include the type of contact, contact name, department, telephone number and e-mail address.

1.4.2 Coordination

List the organizations that may require coordination between the project and its specific support function (e.g., installation coordination, security, etc.). Include a schedule for coordination activities.

1.4.3 Help Desk

Provide help desk information including the responsible personnel's phone numbers for emergency assistance.

1.5 Glossary

Supply a glossary of all terms and abbreviations used in this document. If the glossary is several pages in length, it may be included as an appendix.

2.0 SYSTEM OPERATIONS OVERVIEW

2.1 Operations

Briefly describe the operation of the system, including its purpose and uses.

2.2 Software Inventory

Provide an inventory of the system's programs. Include each program's full name and identification, as well as the security characteristics of the software. Identify those programs necessary to continue or resume operation of the system in a degraded or an emergency situation. Also document how these various programs communicate with each other (API) and with the outside world.

2.3 Information Inventory

Present an overview of the system information and the retention requirements information for these inventories as follows:

- Resources – List permanent files and databases that are referenced, created or updated by the system. Include the files and database names, specific file identification, storage media and required storage capacity, as well as security considerations. Identify those files and databases necessary to continue or resume system operation in a degraded or an emergency situation;
- Reports – List all system generated reports. Include the following information for each report:
  - Security considerations;
  - Media (hard copy, electronic media);
  - Frequency of reporting;
  - Typical report volume;
  - Software that produces the report, if applicable.

2.4 Operational Inventory

Identify any infrastructure hardware and/or software support related to the system operation, including the peripheral and resource requirements (e.g., network management software).

2.5 Processing Overview

Provide information that is applicable to the processing of the system in respect to:

- Interfaces – Describe operational interfaces to other systems (e.g., input data for this system comes from the same source and on the same physical media shared by another system);
- Restrictions – Identify any system restrictions imposed on this system (e.g., times of day when system can be run);
- Waivers of Operational Standards – Describe any waivers that are, or will be, filed to exempt the operation of the system from operational standards already followed.

2.6 Communications Overview

Describe, or depict, the communications network necessary to operate the system. Detail the network topology by diagramming specific devices at each node, by brand, mode and serial number (if necessary.)

2.7 Security

Discuss the system's security considerations. This may include the induction/exit procedures to follow when someone is hired/fired.

3.0 RUN INFORMATION

Here you may describe the runs for use by operations and scheduling personnel in efficient scheduling of operations, assignment of equipment, the management of input and output data, and restart/recovery procedures.

3.1 Inventory

List the runs showing software components, the job control batch file names, run jobs and purpose of each run if any portion of the system is run in batch mode. For online transaction-based processing, provide an inventory of all components that must be loaded for the software system to be operational.

3.2 Description

Provide detailed information needed to execute the system runs. Organize the information in a manner most useful to the IT personnel responsible for system execution. Each run should be under a separate section header, 3.2.1 - 3.2.x.

3.2.x [Run Identifier]

Provide a run identifier for reference in the remainder of the subsection. Describe the run, including, at a minimum, the following:

- Descriptions of all related files and databases
- Estimated run time (in computer units)
- Job dependencies
- Method of initiation (on request, initiation by another run, predetermined time)
- Purpose of each run
- Required turnaround time
- Requirements and procedure for report generation and reproduction
- Run listing and operation schedule
- Run management requirements
- Run stream job control statements for job initiation.

3.2.x.1 Run Interrupt Checkpoints

Identify and describe the acceptable system interrupt points to permit the manual or semiautomatic verification of intermediate results, to provide the user with intermediate results for other purposes or to permit a logical break if higher priority jobs are submitted.

3.2.x.2 Set-Up and Diagnostic Procedures

Provide the set-up and procedures for any software diagnostics. Relate to individual software units, if applicable. Include procedures for validation and troubleshooting. Explain all parameters (both input and output), codes, and range of values for diagnostic software.

3.2.x.3 Error Messages

List all error messages and the corresponding correction procedure for each message. Relate to the specific software units, if applicable.

3.2.x.4 Restart/Recovery Procedures

Provide information to the IT personnel regarding restart/recovery procedures that those persons will follow in the event of system failure. Outline the sequence(s) in which devices and services need to be started under various conditions (e.g. power failure, cold boot, warm boot etc.) Also, define the procedures and sequences for rebuilding the machine(s), if necessary.

3.2.x.5 Problem Reporting/Escalation Procedure

Provide instructions for reporting problems to a point of contact. Include the person's name and phone numbers (that is, office, home, pager, etc.).

GSA System Administration Manual

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

A Systems Administration Manual serves the purpose of an Operations Manual in distributed (client/server) applications.

1.0 GENERAL

1.1 Introduction and Purpose

This section introduces and describes the purpose of the Systems Administration Manual, the name of the system to which it applies, and the type of computer operation.

1.2 Project References

This section lists, at a minimum, the User Manual, Maintenance Manual, and other pertinent available systems documentation.

1.3 Glossary

This section lists all definitions or terms unique to this document or computer operation and subject to interpretation by the user of this document.

2.0 SYSTEM OVERVIEW

2.1 System Application

This section provides a brief description of the system, including its purpose and uses.

2.2 System Organization

This section describes the organization of the system by the use of a chart depicting components and their interrelationships.

2.3 Information Inventory

This section provides information about data files, and the databases that are produced or referenced by the system.

2.3.1 Resource Inventory

This section lists all permanent files and databases that are referenced, created, or updated by the system.

2.3.2 Report Inventory

This section lists all reports produced by the system, including each report name and the software that generates it.

2.4 Processing Overview

This section provides information that is applicable to the processing of the system. It includes system restrictions, waivers of operational standards, and interfaces with other systems.

2.5 Communications Overview

This section describes the communications functions and process of the system.

2.6 Security

This section describes the security considerations associated with the system.

2.7 Privacy Act Warning

If this system is covered by the Privacy Act, then this section provides the appropriate Privacy Act notice and warning.

3.0 SITE PROFILE(S)

This section contains information pertaining to the site(s) where the application is running. That information includes the information contained in the subsequent sections.

3.1 Site Location(s)

This is the official address(es) of the site(s).

3.2 Primary Site

For the site(s) designated as primary, this section describes the essential personnel names and phone numbers for the automated data processing site contacts.

4.0 SYSTEMS ADMINISTRATION

This section introduces the responsibilities of the System Administrator, as discussed in the subsequent sections.

4.1 User and Group Accounts

This section introduces topics related to system users.

4.1.1 Adding/Deleting Users

This section describes procedures to create/delete user logins and password accounts.

4.1.2 Setting User Permissions

This section describes procedures to give users/restrict access to certain files.

4.1.3 Adding/Deleting User Groups

This section contains procedures to create/delete user groups.

4.1.4 Setting User Roles/Responsibilities

This section describes the roles that are granted to each group or individual user(s).

4.2 Server Administration

This section describes procedures to setup servers, including naming conventions and standards.

4.2.1 Creating Directories

This section describes procedures to create server directories, and a complete description of the existing directories.

4.2.2 Building Drive Mappings

This section describes procedures to create server drive mappings, and a complete description of the existing drive mappings.

4.3 System Backup Procedures

This section describes procedures for regularly scheduled backups of the entire network, including program and data storage, and the creation and storage of backup logs.

4.3.1 Maintenance Schedule (Daily, Weekly)

This section describes documented daily and weekly backup schedules and procedures. The procedures should include tape labeling, tracking, and rotation instructions.

4.3.2 Off-Site Storage Procedures

This section describes the location, schedule, and procedures for off-site storage.

4.3.3 Maintaining Backup Log

This section describes procedures for creating and maintaining backup logs.

4.4 Printer Support

This section discusses procedures for installing, operating, and maintaining printers.

4.4.1 Maintenance (Configurations, Toner, Etc.)

This section describes maintenance contracts, procedures to include installation and configuration of printer drivers, and equipment information.

4.4.2 Print Jobs (Moving, Deleting, Etc.)

This section describes procedures to monitor, delete, and prioritize print jobs.

4.5 System Maintenance

This section discusses procedures for maintaining the file system.

4.5.1 Monitoring Performance and System Activity

This section contains procedures to monitor system usage, performance, and activity. This may include descriptions of system monitoring tools, the hours of peak demand, a list of system maintenance schedules, etc.

4.5.2 Installing Programs and Operating System Updates

This section includes procedures on how to install and test operating system updates. Once tested, instructions are to be provided to move/install the operating system updates to the operational environment.

4.5.3 Maintaining Audit Records of System Operation

This section describes procedures for the setup and monitoring of the operating system and application audit trails.

4.5.4 Maintenance Reports

This section includes procedures to create and update maintenance reports.

4.6 Security Procedures

This section describes the process for obtaining identifications (IDs) and passwords. It includes information concerning network access and confidentiality requirements.

4.6.1 Issuing IDs and Passwords

This section describes procedures for issuing IDs and passwords for operating systems and applications.

4.6.2 License Agreements

This section describes licensing agreements and procedures for ensuring that all licenses are current.

4.7 Network Maintenance

This section describes procedures to maintain and monitor the data communications network.

4.7.1 LAN Design

This section contains a layout of the network.

4.7.2 Communications Equipment

This section contains a layout of the telecommunications equipment.

4.8 Inventory Management

This section contains a complete hardware and software inventory to include make, model, version numbers, and serial numbers.

4.8.1 Maintaining Hardware and Software Configurations

This section describes procedures for maintaining the configuration information for the hardware and software actually installed.

4.8.2 Maintaining Floor Plans

This section describes procedures for maintaining floor plans showing the location of all installed equipment and how to add/delete/modify the plans.

4.8.3 Installing Software/Hardware (New, Upgrades)

This section describes procedures for installing new or upgrading hardware and software.

4.8.4 Maintaining Lists of Serial Numbers

This section describes procedures for maintaining all serial number lists required at the site.

4.8.5 Maintain Property Inventory

This section describes procedures for maintaining a property inventory at the site.

4.9 Training Backup Administrator

This section describes how to train a backup administrator.

4.10 End-User Support–Procedures for Support and Contract Information

This section provides necessary end-user contract information and the procedures for providing end-user support.

4.10.1 Escalation Procedures

This section describes the formal escalation procedures to be used by System Administrators in response to priority user problem resolution requests.

4.11 Documentation

This section describes the documentation required of System Administrators as they perform system administration.

4.11.1 Troubleshooting Issues

This section describes how to conduct and document troubleshooting activities.

4.12 Database Maintenance

This section introduces the responsibilities as they relate to the database and software application maintenance.

4.12.1 Database User/Group Access

Describe who provides database access and the procedures for granting access.

4.12.2 Adding/Deleting Users to Database

Provide the responsible person who adds and deletes users to the database. Include the procedures for adding/deleting users.

4.12.3 Setting User Permissions for Database

Provide the responsible person who sets the permissions for users on the database.

4.12.4 Adding/Deleting Groups for Database

Provide the procedures and responsible person for adding/deleting groups of individuals to the database.

4.12.5 Re-indexing Database

Provide the procedures and responsible person for re-indexing the database after changes have been made.

4.12.6 Packing/Compressing Database

Provide the procedures and responsible person for packing/compressing the database.

4.12.7 Data Entry/Modification/Deletion

Provide the responsible person(s) who can make changes to the database. Include procedures for data entry, modifying, and deleting information from the database.

4.12.8 Database Reporting

Provide the responsible person(s) for database reporting. Include what reports are generated, time frames, due dates and storage of the reports.

4.12.9 Database Backup and Restore

Provide the person(s) responsible for performing database backup. This information should also be included in the Contingency Plan. Include procedures to follow if the database needed to be restored.

4.13 Application Maintenance

4.13.1 Application User/Group Access

Describe who provides application access and the procedures for granting access.

4.13.2 Adding/Deleting Application users

Provide the responsible person who adds and deletes users to the application. Include the procedures for adding/deleting users.

4.13.3 Setting User Application Permissions

Provide the responsible person who sets the permissions for users of the application.

4.13.4 Adding/Deleting Application Groups

Provide the procedures and responsible person for adding/deleting application groups.

4.13.5 Procedures to Start and Stop the Application

Provide who has responsibility to start and stop the application. Include a rationale for stopping the application, and the steps to take to restart after identified problems are corrected.

4.13.6 Application Flow Chart

Provide a flow chart depicting how the information moves from the application to the database.

4.13.7 Description of Major Program or Sub-program Modules

Describe the processes within the application or module. If more than one module is operating for this system, describe each module.

Training Plan *(TP)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

TRAINING PLAN

EXECUTIVE SUMMARY

The Training Plan (PT) defines the support activities, schedules, curriculum, methods and tools and the equipment required for the system training. PT is prepared either as a separate, or as part of the Project Plan, document and also covers the coordination of training schedules, reservation of the personnel and facilities, planning for training needs and other training-related tasks.

1.0 INTRODUCTION

1.1 Purpose

The purpose of PT should be provided here (Similar text as the Executive Summary, above, can be used.)

1.2 System Overview

Provide an overview of the system as follows:

- Responsible Organization
- General Description
- Category, Code and Name/Title
- Environment or special conditions
- Operational Status (D/M/E or O&M)
- System Architecture --in non-technical terms-- (e.g., client/server, web-based, etc.)
- Training Prerequisites –brief– for each type of training mentioned in the PT document.

1.3 Project References

Provide a list of references that were used in preparation of this document. This should, at a minimum, include the Project Plan, FRD, SDD, CP, Test Plan, and the IP documents.

1.4 Points of Contact

List the organization name/code and title of key points of contact (POCs) for system development. This list should include –if applicable-- such POCs as the Project Lead, Program Manager, QA Manager, Security Manager, Training Coordinator, and the Training Representative(s). For each POC, provide the following:

- Type
- Name
- Department
- Telephone Number
- E-mail address (if applicable)

1.5 Glossary

Supply a glossary of all terms and abbreviations used in this document. If the glossary is several pages in length, it may be included as an appendix.

2.0 REQUIREMENTS TRACEABILITY OPTIONAL

If applicable, present the RVTM (from the previously developed FRD document) that lists the users' requirements and traces how they are addressed in the SDD, TP and PT. Cross-reference the users' requirements and training needs in the appropriate sections of the PT.

The RVTM may be broken into segments. For example, provide a separate matrix of the PT sections that trace to particular sections in the FRD, SDD and the SOW.

3.0 TRAINING PREREQUISITES

3.1 Target Audience(s)

Discuss the training course's target audience(s). This may span a wide spectrum ranging from the data entry and clerical staff members on one end to highly specialized professionals (users, technical, IT and non-IT managers and executives) at the other. The tasks that must be taught to meet objectives successfully and the skills that must be learned to accomplish those tasks should be described here. Also in this section, the training needs for each target audience, as well as the needs in terms of staff location groupings such headquarters and field offices, can be presented

3.2 Tailored Training Approach

Present the approach used to develop specialized course curriculum tailored to each target audience needs and ensure quality training products. This description should include the methodology used to analyze training requirements in terms of performance objectives and to develop course objectives that ensure appropriate instruction for each target group. The topics or subjects on which the training must be conducted should be listed or identified.

3.3 Issues and Recommendations

All current and foreseeable issues surrounding training should gain visibility. Recommendations for resolving each issue and constraints and limitations should also be thoroughly discussed here.

4.0 TRAINING APPROACH

4.1 Methodology

Describe the training methods to be used in the proposed courses; these methods should relate to the needs and skills identified in 3.1 above, and should take into account such factors as course objectives, the target audience, media characteristics, training setting criteria and costs. The materials for chosen training approach, such as course outlines, audiovisual aids, instructor and student guides, student workbooks, examinations and reference manuals should be listed or discussed in this section.

4.2 Tools

These techniques may include computer-based instruction, self-paced written manual, peer training, hands-on practical sessions, classroom lectures or any combination of the above.

4.3 Database

If applicable, identify and discuss the training database and its usage during the training. Describe the simulated production data related to various training scenarios and cases developed for instructional purposes. Also explain how the training database will be developed.

5.0 TRAINING RESOURCES

5.1 Course Administration

Describe the methods used to administer the training, including the procedures for class enrollment, student release, reporting of academic progress, course completion and certification, monitoring of the training program, training records management and security, as required.

5.2 Resources and Facilities

Elaborate on the training resources required by instructors and students, including classroom, training, and laboratory facilities; equipment such as an overhead projector, projection screen, flipchart or visual aids panel with markers, and computer and printer workstations; and materials such as memo pads and pencils, diskettes, viewgraphs and slides. Information contained in this section can be generic in nature and can apply to all courses. Specific course information and special needs may be itemized here or in paragraph 6.0 below.

5.3 Schedules

Prepare a training schedule to include the following information:

- Identification and the development time-line of course content and materials
- Planned training dates
- Post training reporting
- Names of students
- Names of instructor
- Location of session

The schedule should be as comprehensive as possible; however, the schedule may be revised at later points in the project lifecycle. In the final version of the PT, actual course schedules by location should be included.

5.4 Future Training

Discuss the scheduled training modifications and improvements. This information can include periodic updating of course contents, planned modifications to training environments, retraining of employees, and other predicted changes. Indicate procedures for requesting and developing additional training.

6.0 TRAINING CURRICULUM

For each course, provide descriptions of the course components. Subsections of this section, should be created for each course.

Each course may comprise one or more modules. A course description should be developed for each module. At a minimum, each course description should include the course/module name; the length of time the course/module will take; the expected class size (minimum, maximum, optimal); the target audience; course objectives; module content/syllabus; specific training resources required, such as devices, aids, equipment, materials, and media to be used; and any special student prerequisites. The course description could also include information on instructor-to-student ratio, total number of students to be trained, estimated number of classes, location of classes, and testing methods.

In lieu of the all above, the course description(s) from the vendor can be attached here.

7.0 EVALUATION

7.1 Metrics

Outline the metrics that will be captured and how they will be captured. Examples of some of the metrics that should be tracked include:

- Total Staff
- Duration (estimated versus actual)
- Number of Attendees (estimated versus actual)
- Percent of Total Attended
- Percent of Estimated Attended
- ....

7.2 Strategy

Describe how feedback will be elicited to establish and maintain the curriculum development process's quality. Include methods used to test and evaluate the training effectiveness, evaluate student progress and performance and apply feedback to modify or enhance the course materials and structure.

One feedback collection mechanism could be that of a course or instructor evaluation form (completed for each course/module). This form should capture –at the minimum-- the trainee(s)' reaction on the following:

- Adequacy of the Facilities;
- Appropriateness of Objectives;
- Effectiveness of Course Training Materials;
- instructor(s)' Effectiveness;
- Participant Suggestions and Comments;
- Scope and Relevance of the Course or Module;
- Stronger/Weaker Course Features;
- Timing/Length of the Course or Module; and
- Usefulness of Assignments and Materials.

User Manual *(UM)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

USERS' MANUAL

EXECUTIVE SUMMARY

The Users' Manual (UM) document provides the information necessary for the users to effectively use a system. It contains description of the system functions and capabilities, contingencies and alternate modes of operation, and step-by-step procedures for system access and usage.

1.0 INTRODUCTION

1.1 Purpose

The purpose of UM should be provided here (Similar text as the Executive Summary, above, can be used.)

1.2 Authorization

Provide a warning regarding the unauthorized usage of the system and making unauthorized copies of data, software, reports and documents. If the usage waivers or copy permissions need to be obtained, describe the process.

1.3 Project References

Provide a list of references that were used in preparation of this document. This should, at a minimum, include the FRD, SDD, CMP and the QAP documents.

1.4 Points of Contact

List the organization name/code and title of key points of contact (POCs) including –if applicable-- the POCs for Development/Maintenance, Help Desk, and Operations. For each POC, provide the following:

- Type
- Name
- Department
- Telephone Number
- E-mail address (if applicable)

1.5 Glossary

Supply a glossary of all terms and abbreviations used in this document.

2.0 SYSTEM SUMMARY

Provide a general system overview written in non-technical terminology. The summary should outline the uses of the system in supporting the activities of the users and staff.

2.1 System Configuration

Briefly describe, and depict graphically, the equipment, communications and networks used by the system. Include the type of computer input and output devices.

2.2 Data Flows

Briefly describe, or depict graphically, the overall flow of data in the system. Include a user-oriented description of the method used to store and maintain data.

2.3 User Access Levels

Describe the different users and/or user groups and the restrictions placed on system accessibility or usage for each.

2.4 Contingencies and Alternate Modes of Operation

On a high level, explain the continuity of operations in the event of emergency, disaster or accident. Explain what the effect of degraded performance will have on the users.

3.0 GETTING STARTED

Provide a general walkthrough from initiation through exit. The logical presentation of the information should enable the functional personnel to understand the sequence and flow of the system. Use screen prints to depict examples of text under each heading.

3.1 Logging In & Out

Describe the procedures necessary to access the system, including how to get a user ID and log on. If applicable, identify job request forms or control statements and the input, frequency, reason, origin and medium for each type of output. Detailed procedures for changing a user ID and/or password and the actions necessary to properly exit the system, must also be included here.

3.2 System Menu

Discuss, in general terms, the very first system menu that a user will see, as well as the navigation paths to functions noted on the screen. Each function should be under a separate section header, 3.2.1 - 3.2.x.

3.2.x [System Function Name]

Provide a function name and identifier here for reference in the remainder of the subsection. Describe the function and pathway of the menu item and include the following, as appropriate:

- Purpose and uses of the function
- Initialization of the function, if applicable
- Execution options associated with this function
- An average response time to use the function
- Description of function inputs:
  - Title and description of each input, including graphic depictions of display screens
  - Purpose and use of the inputs
  - Input medium
  - Limitations and restrictions
  - Format and content on inputs, and a descriptive table of all allowable values for the inputs
  - Sequencing of inputs
  - Special instructions
  - Relationship of inputs to outputs
  - Examples
- Description of expected outputs and results:
  - Description of results, using graphics, text, and tables
  - Form in which the results will appear
  - Output form and content
  - Report generation
  - Instructions on the use of outputs
  - Restrictions on the use of outputs, such as those mandated by Privacy Act and Computer Security Act restrictions
  - Relationship of outputs to inputs
  - Function-specific error messages
  - Function-specific or context-sensitive help messages associated with this function
- Relationship to other functions
- Summary of function operation.

4.0 ON-LINE USAGE

Provide a detailed description of system functions. Each function should be under a separate section headers: 4.1 - 4.x, and correspond sequentially to the system functions listed in subsections 3.2.1 - 3.2.x.

4.x [System Function Name]

Provide a function name and identifier here for reference in the remainder of the subsection. Describe the function in detail and depict graphically. Include screen captures and descriptive narrative.

4.2 Instructions for Error Correction

Describe all recovery and error correction procedures, including error conditions that may be generated and corrective actions that may need to be taken.

4.3 Caveats and Exceptions

If there are special actions the user must take to insure that data is properly saved or that some other function executes properly, describe them here (Include screen captures and descriptive narratives, if applicable.)

5.0 BATCH USAGE

Provide a detailed description of system functions. Each function should be under a separate section headers: 5.1 - 5.x, and correspond sequentially to the system functions listed in subsections 3.2.1 - 3.2.x.

5.x [System Function Name]

Provide a function name and identifier here for reference in the remainder of the subsection. Describe the function in detail and depict graphically. Include screen captures and descriptive narrative.

5.2 Instructions for Error Correction

Describe all recovery and error correction procedures, including error conditions that may be generated and corrective actions that may need to be taken.

5.3 Caveats and Exceptions

If there are special actions the user must take to insure that data is properly saved or that some other function executes properly, describe them here (Include screen captures and descriptive narratives, if applicable.)

5.4 Input Procedures and Expected Output

Prepare a detailed series of instructions (in non technical terms) describing the procedures the user will need to follow to use the system. The following information should be included in these instructions:

- Detailed procedures to initiate system operation, including identification of job request forms or control statements and the input's frequency, reason, origin and medium for each type of output
- Illustrations of input formats
- Descriptions of input preparation rules
- Descriptions of the output procedures identifying formats and specifying the output's purpose, frequency, options, media and location
- Identification of all codes and abbreviations used in the system's output.

6.0 QUERIES

Discuss the query and retrieval capabilities of the system. The instructions necessary for recognition, preparation and processing of a query applicable to a database should be explained in detail. Use screen prints to depict examples of text under each heading.

6.1 Capabilities

Describe or illustrate the system's pre-programmed and ad hoc query capabilities. Include query name or code the user would invoke to execute the query and the query parameters (if applicable.)

6.2 Procedures

Develop detailed descriptions of the procedures necessary for file query including the parameters of the query and the sequenced control instructions to extract query requests from the database.

7.0 REPORTS

Present all standard reports that can be generated by the system or internal to the user. Use screen prints as needed to depict examples of text under each heading.

7.1 Capabilities

Describe all reports available to the end user. Include report format and the meaning of each field shown on the report. If user is creating ad hoc reports with special formats, describe here. A separate subsection may be used for each report.

7.2 Procedures

Provide instructions for executing and printing the different reports available. Include descriptions of output procedures identifying output formats and specifying the output's purpose, frequency, options, media, and location.

IT Contingency Plan

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

EXECUTIVE SUMMARY

By definition, a Contingency Plan (CP) is: "A plan involving suitable backups, immediate actions and longer term measures for responding to emergencies such as attacks or accidental disasters. Contingency plans are part of the business resumption planning."

The process of developing a CP involves convening a team representing all sectors of the organization, identifying critical resources and functions and establishing a plan for recovery based on how long the enterprise can function without specific functions. Being a "living" document, the CP must be documented and tested until it works effectively.

Preparation for handling contingencies/disasters is known by contingency planning, though it has other names like: *disaster recovery, business continuity, continuity of operations (CoOp), or business resumption, planning.*

1.0 INTRODUCTION

1.1 Purpose & Scope

OMB A-130 mandates the preparation of plans for general support systems and major applications to ensure the continuity of operations.

This CP which is intended to address the major applications part of the OMB requirements, identifies the critical business functions needed to ensure the availability of essential services and programs, as well as the plan for post-disaster recovery (i.e., which applications should be restored first).

1.2 System Overview

Describe the basic functions and outputs of the system. Continue by detailing the systems' or process specifics:

- Current Platform or Technology – Include hardware, software and networking information;
- Interfaces with Other Systems;
- Critical Processes and Outputs – Include reports and other outputs; and
- Key Contact Information for the personnel who have system/process responsibility and have a good working knowledge of the system:
  - Area of Expertise/Specialty
  - Name
  - Department
  - Telephone Number and/or E-mail address (if available)

1.3 Assumptions

A CP is based on several categories of assumptions. Most can be established only after the completion of a risk assessment (reference the Security Risk Assessment document here.) The entire list of assumptions for inclusion in the document cannot be completed until well along in the planning cycle. Included in the set of assumptions should be the following:

- Nature of the Problem
- Priorities
- Commitments to or Assumptions of Support.

1.4 Contingency Plan's Objectives

1.4.1 Risks of Failure

Discuss the risk of failure. Include a copy of the risk rating form or other risk evaluation documentation. Describe the risk and how would it impact the organization.

1.4.2 Risk of Contingency Plan

Describe what the risks are involved with using the chosen CP and how it might impact the organization.

1.4.3 Desired Outcomes

Present the desired outcomes in terms of output and level of service? How long do we plan to operate under the contingency mode?

1.4.4 Potential Impact

Describe the anticipated impact on the organization in lower service or functional levels. This should include descriptions of potential impact in terms of financial, customers and good will costs.

1.5 Glossary

Supply a glossary of all terms and abbreviations used in this document.

2.0 CP STRATEGY

Selection of a meaningful CP strategy must always follow the risk assessment. Until the risk assessment is completed, it is hard to know the criticality of the systems that must be maintained and the demands for the resources necessary for such support.

2.1 Identify Resources

The CP needs to be developed by a team representing every single functional area of an organization. If the organization is large enough, a formal project needs to be established, which must have approval and support from the very top of the enterprise. For each resource, provide the following estimates:

- Time – Required to implement the plan. Remember the approval processing time for necessary spending authorization and procurement processing.
- Cost – This is the plan's budget for the cost of equipment, supplies, services, staff overtime etc.

2.2 Prepare Incidents List

Assuming that the risk assessments are completed, and based on the results, one of the first CP tasks to be undertaken is to prepare a comprehensive list of the potentially serious incidents that could affect the normal operations of the business. This list should include all the possible incidents no matter how remote the likelihood of their occurrence appears to be.

2.3 Weigh Individual Incidents

Against each item listed the project team or manager should note a probability rating. Each incident should also be rated for potential impact severity level. From this information, it will become much easier to frame the plan in the context of the real needs of the organization.

3.0 CP IMPLEMENTATION

Once the assessment stage has been completed, the structure of the plan can be established. The plan will contain a range of milestones to move the organization from its disrupted status towards a return to normal operations.

The first major milestone is the process dealing with the immediate aftermath of the disaster. This may involve the emergency services or other specialists who are trained to deal with extreme situations. The next stage is to determine which critical business functions need to be resumed and in what order. The CP should be detailed, and identify key individuals who should be familiar with their duties under the plan.

3.1 Implementation Criteria

Describe the basic criteria for implementing the CP. What will be the situation that prompts the decision to implement?

3.2 Trigger Events

Identify the date or specific failure that will trigger the CP implementation. You may want to describe the various scenarios that could lead to a trigger event.

3.3 Responsibilities

Who is responsible for making the implementation decisions? If you have a clearly documented trigger event this could be whoever is on duty at the time the event happens.

3.4 Duration

What is the estimated length of time that contingency operations will cover?

4.0 OPERATION & MANAGEMENT UNDER CONTINGENCY

4.1 People

Humans are the most critical elements in the recovery from damaging losses. To the degree necessary, describe the personnel structure that will be used to ensure smooth operations under contingency plan:

- Decision Makers who will make decisions to implement, change or discontinue the contingency;
- Support Personnel who will be used to implement and operate processes under the plan.

4.2 Roles and Responsibilities

Provide details on what each team will do what under the plan:

- Emergency Response Teams;
- Contingency Operations Teams.

4.3 Notification Procedures

Discuss the plan to notify the staff of the CP implementation. Given the possibility of telecommunication disruptions, you may want to have an automatic response (in the event the phones go dead or the power goes out) or have teams standing by at critical times and dates.

4.4 Records Management Procedures

Describe how you plan to manage records issues. Consider reports and data dumps that will be useful in the recovery phase.

4.5 Data Security Procedures

Describe the processes to be employed to ensure data security, recovery, integrity and confidentiality. CPs may open the door to significant security issues. Review systems security and access rights, data integrity assurance procedures and records confidentiality procedures.

5.0 RETURNING TO NORMAL OPERATIONS

Elaborate on how you will determine that it is time to discontinue the contingency mode and return to the normal operation mode.

5.1 Criteria

Describe the conditions or events that would lead to returning to normal operating mode. This should include certification that the system or process is functioning normally.

5.2 Procedures

Describe the detailed procedures required to return to normal operating mode.

5.3 Recovery Processes

Describe the process, requirements and the steps to be taken to recover data and bring the processes bask to normal. Be as specific as necessary.

5.4 Points of Contact/Notifications

List key personnel with responsibility for returning the system/process to its normal operating mode:

- Decision-Makers for continue-return decisions;
- Operational Personnel that will be needed to return to normal operations;
- Business Recovery Team that will lead the process of resuming normal operations (after contingency);

- Business Partners (internal and external) that will be involved in resuming normal operations.

6.0 TRAINING & TESTING

Training may include desktop exercises and rehearsals to ensure the smooth implementation of the CP. Testing is used to validate the CP's capabilities. Provide specifics for the following:

- Contingency Team Training – Will they need to be trained on new or different processes? Will they need to practice manual operation scripts? Will you include a drill?
- Recovery Team Training required for the team that will bring processes back on line;
- Testing Requirements and Procedures. For ensuring the completeness of the CP (include test scripts and other detailed testing procedures);
- Training & Testing Schedules (including timelines) to ensure readiness of both staff and the CP prior to implementation.

7.0 CP MAINTENANCE

The CP must always be kept up to date and applicable to current business circumstances. This means that any changes to the business process or changes to the relative importance of each part of the business process must be properly reflected within the CP.

Someone must be assigned the full responsibility for ensuring that the CP is maintained and updated regularly and should therefore ensure that information concerning changes to the business process is properly communicated.

Any changes or amendments made to the CP must be fully [re]tested. Personnel should also be kept abreast of such changes in so far as they affect their duties and responsibilities.

Test Analysis Report *(TAR)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

TEST ANALYSIS REPORT

EXECUTIVE SUMMARY

According to the FAS' verification and validation (V&V) plan document, a Test is:

"... the act of using real or simulated inputs to show that a product satisfies its requirements and, if it does not, to identify the specific differences between the expected and actual results."

It further recognizes several levels/stages of testing, namely:

- Component Testing
- Integration Testing
- System Testing
- Acceptance Testing

The Test Analysis Report (RT) records results of the tests --at any level--, presents the capabilities and deficiencies for review and provides the means for assessing the progression to the next stage of development and/or testing.

1.0 OVERVIEW

1.1 Purpose

The RT documents the results of system testing and provides a basis for assigning responsibility for deficiency correction and follow-up.

1.2 Background

Provide a description of history and other background leading up to the current round of testing. Identify the user organizations and the location where the testing took place. Describe any prior testing and note the results that may have affected this testing.

1.3 Scope

Present the testing scope. Note the:

- Functionality/Features/Behavior that were tested
- Functionality/Features/Behavior that were not tested.

1.4 Project References

Provide a list of documents and guidance material that were referenced and/or used during the course of testing. This should, at a minimum, include the FRD (RVTM,) OM, MM, UM, and the Test Plan documents.

1.5 Limitations and Constraints

Detail any business, product line or technical constraints that impacted the conduct of the testing. Also, identify limitations that were imposed on the testing, whether due to lack of specialized test equipment, or of time or resources. Indicate the steps that were taken to reduce the impact of such limitations(s).

1.6 Glossary

Provide definitions for terms and acronyms used in the TP document.

2.0 TEST ANALYSIS

Identify the tests being conducted and provide a brief description of each. Each test in this section should be under a separate section header (Generate new sections as necessary for each test from 2.2 - 2.x.)

2.1 Security Considerations

Detail the security requirements that have been built into the system and verified during the acceptance testing. Identify and describe security issues or weaknesses that were discovered as a result of testing.

2.x [Test Identifier]

The tests in sections 2.2 through 2.x of this RT should correspond to the tests described in sections 3.1 through 3.x of the Test Plan document.

Provide a test name and identifier for reference in the remainder of the section. Identify the functions that were tested and are the results of which are being reported. Include the following information when recording the results of a test:

- Name and version number of the application or document that was tested;
- Identification of the input data used in the test (e.g., file ID);
- Identification of the hardware and operating systems on which the test was run;
- Time, date and location of the test;
- Names, work areas, email addresses and phone numbers of personnel involved in the test;
- Identification of the output (e.g., file ID) data, with detailed descriptions of any deviations from the expected outcome.

2.x.1 Expected Outcome

Describe or illustrate the expected test result of the test.

2.x.2 Functional Capability

Describe the capability to perform the function as it has been demonstrated. Assess the manner in which the test environment may be different from the operational environment and the effect of this difference on the capability.

2.x.3 Performance

Quantitatively compare the performance characteristics of the system with the FRD requirements.

2.x.4 Deviations

Describe any deviations from the original V&V and Test Plan that occurred during the test. List reasons for the deviations.

3.0 CONCLUSION

3.1 Demonstrated Capability

Provide a general statement of the system's capability as demonstrated by the test, compared with the FRD requirements and security considerations. An individual discussion of conformance with specific requirements must be cited.

3.2 System Deficiencies

Present an individual statement for each deficiency discovered during the testing. Accompany each deficiency with a discussion of the following:

- Names, work areas, email addresses and phone numbers of development area personnel who were informed about the deviations;
- Date the developers were informed about the potential problem;
- Date the new version was reissued;
- If the deficiency is not corrected, the consequences to operation of the system;
- If the deficiency is corrected, the responsible organization and a description of the correction (path #, version, etc.)

3.3 Recommended Improvements

Provide a detailed description of any recommendation discovered during the testing that could improve the system, its performance or its related procedures. If an additional functionality is seen as a potential improvement for the user, but is outside the FRD, it should be included here. Provide a priority ranking of each recommended improvement relative to all suggested improvements for the system.

3.4 System Acceptance

State whether the testing has shown that the system is ready for release to the production environment.

Post Implementation Report *(PIR)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

POST-IMPLEMENTATION REVIEW

EXECUTIVE SUMMARY

A Post-Implementation Review (PIR) is an assessment and review of the completed working solution. It will be performed after a period of live running. In simple terms, it asks the question "did we achieve the benefits set out in the business case?" and proceeds by answering the question along with presenting outlooks for future endeavors based on lessons-learned from the freshly-implemented system.

Therefore, it is imperative to use the review findings constructively not just for the benefit of this project, but as importantly, the lessons-learned for the future projects.

A PIR should be scheduled some time after the solution has been deployed. Typical periods range from 6 weeks to 6 months, or until at least one full processing and reporting cycle has been completed. It should not be performed while the initial snags are still being dealt with or while users are still being trained, coached and generally getting used to its operation.

The PIR should be timed to allow the final improvements to be made in order to generate optimum benefit from the solution. There is no point in waiting too long as the results are intended to generate that final benefit for the organization and team.

1.0 OVERVIEW

1.1 Purpose

There are three purposes for a PIR:

- To ascertain the degree of success from the project, in particular, the extent to which it met its objectives, delivered the planned levels of benefit and addressed the specific requirements;
- To examine the efficacy of all elements of this working solution to see if further improvements can be made to optimize the delivered benefits; and
- To learn lessons from this project, lessons which can be used by the team members and by the organization to improve future working and solutions.

1.2 Background

Provide the following background information for the system leading up to its current implementation:

- Project Name
- Project Summary
- Name of Responder – Enter the name of the person completing the survey (PIR)
- Responder's Project Role – Common roles include:
  - Business Analyst
  - Developer
  - Project Manager
  - Project Team Member
  - Sponsor
  - Stakeholder
  - Technical Analyst
  - Tester
  - User

2.0 PIR PARAMETERS

2.1 Schedule

In regards with the implementation's timeliness and the scheduling, the PIR responder should answer the following questions:

- Did the project remain on schedule?
- What helped the project remain on schedule?
- What prevented the project from remaining on schedule?
- What strategies were used to help the project stay on schedule?

2.2 Costs

In regards with the implementation's cost-effectiveness, the PIR responder should answer the following questions:

- Did the project remain within predicted budget?
- If the project came in under budget, how were savings made?
- If the project ran over budget, why did this happen?

2.3 Goals & Objectives

In regards with the implementation's goals, the PIR responder should answer the following questions:

- What were the major goals & objectives of this project?
- Did the project deliverables align with these goals and objectives?
- Did project outcomes help meet the goals and objectives?
- If not, why did the project vary from the objectives?

2.4 Requirements & Functionality

In respect to the implemented system's capability to meet the stated requirements and functionality, the PIR responder should answer the following questions:

- Was the functionality promised as part of this project delivered at the end of the project?
- What was not delivered and what might have caused this?
- Were service requirements met upon project completion?
- If requirements were not met, what caused this?
- Does the system work as intended?

2.5 Benefits

In respect to the implemented system's providing of the perceived/expected benefits, the PIR responder should answer the following questions:

- Do the projected benefits match the actual benefits?
- Are there intangible benefits because of this project?

3.0 FINDINGS & CONCLUSION

3.1 Lessons Learned

The PIR responder should answer the following questions:

- Overall, was the project a success?
- What was done really well?
- What could have been done better?
- What recommendations would you make for future project application?
- What would you do differently if you could do it over again?
- What have you learned that can be applied to future projects?

3.2 Recommendations

The PIR responder should answer the following questions:

- Do you have any advice for future projects?
- Did this project uncover or prove any Best Practices?

3.3 Next Steps

The findings and recommendations will be presented to:

- Solution's Business Owners,
- Leading Participants in the project, and

- Other Parties who may be concerned with the results.

Specific actions should be proposed to address any further recommended work. This might be handled in several different ways, for example:

- As routine support and maintenance,
- As remedial work to be performed by the original project team,
- For line management to address through user education and procedures etc,
- As further phases of development involving new projects.

Disposition Plan *(DP)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

yyyy/mm/dd

December 13, 2006

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006

EXECUTIVE SUMMARY

to an information system from all computer operating platforms and notification of other offices who keep records of computer applications that a system has been disposed.

The objectives of the DP, therefore, are to end the operation or the system in a planned, orderly manner to ensure that system components and data are properly archived or incorporated into other systems. At the end of this task, the system will no longer exist as an independent entity.

The software, hardware and data of the current system are disposed of in accordance with organization needs and pertinent laws and regulations. The DP, however, may not include the removal of information systems from the software libraries used for software reuse and sharing.

The procedure for the DP guidelines is initiated by the Chief Information Officer (CIO) for adoption by all FAS organizations that may be involved in a system disposition.

1.0 OVERVIEW

1.1 Purpose & Scope

The DP procedures establish the processes for orderly disposition of both classified and unclassified information systems, regardless of software platform or size.

Define decommissioning and disposing of the candidate system, equipment and support functions. Prescribe criteria that must be addressed by government and government contractors supporting these systems. Also provide guidelines for the disposal notification process.

1.2 Assumptions

List all the assumptions that have been made in developing this DP.

1.3 Points of Contact

Identify your points of contact (POCs). Provide the name of the responsible organization and staff (and alternatives, if applicable) who serve as the system disposal POCs. Also identify the roles for the government and industry partner key contacts.

1.4 Project References

Present the key project references and/or deliverables that have been produced before this point in the project development. These documents may have been produced in a previous development life cycle that resulted in the initial version or subsequent enhancement efforts of the system, or reference material for the development of this DP.

1.5 Glossary

Provide definitions for terms and acronyms used in the DP document.

2.0 SYSTEM DISPOSITION

2.1 Notifications

Describe the plan for notifying known users of the candidate system’s shutting down, and other affected parties, such as those responsible for other interfacing systems and the operations staff involved in running the system.

2.2 Data

Discuss the plan for archiving, deleting or transferring to other systems, the disposal candidate system’s data files and their related documentation.

2.3 Software

Present the plan for archiving, deleting or transferring to other systems, the disposal candidate system’s software library files and their related documentation.

2.4 System Documentation

Provide the plan for archiving, deleting or transferring to other systems, the disposal candidate system's hardcopy and softcopy systems and user documentations.

2.5 Equipment

Detail the plan for archiving, salvaging or transferring to other systems, the disposal candidate system's hardware and other equipments.

3.0 PROJECT SHUTDOWN

3.1 Staff

Elaborate on how you plan to notify the project team members of the shutdown of the system, and the transfer of these team members to other projects.

3.2 Project Activities

Describe the plan for archiving, deleting, or transferring to other projects, the project activity records for the project that has been maintaining the disposal candidate system.

3.3 Facilities

Present the plan for transferring or disposing of facilities used by the disposal candidate system's staff.

Project Management Plan *(PMP)*

(Version 2.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

mm/dd/yyyy

February 1st, 2012

Table of Contents

Table of Figures

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Release	February 2006
Version 2.0	Revised per FAS/OCIO guidance and PMO recommendations	February 1st, 2012

INTRODUCTION TO THE PMP TEMPLATE DOCUMENT

Project management provides an integrated framework for project organization, planning, execution, and control, and is designed to:

- Ensure the timely and cost-effective production of all the end-products;
- Maintain acceptable standards of quality; and
- Ensure the organization achieves its projected return on investment.

This Project Management Plan (PMP) Template is the reference document for each project to use in creating a specific PMP and is in support of FAS OCIO Systems Development Lifecycle (SDLC).

AUDIENCE

Any stakeholder of the project, who need to know the project plan, and/or expected out comes, or who may be affected by the project; such as Project Managers, Customers, and Contractors/Vendors may be benefited from this document.

HOW THIS PMP TEMPLATE SHOULD BE USED

This PMP Template should be used as a guide for creating a project unique PMP. This document is subject to tailoring to accommodate project specific needs. All parts of this document may not apply to every project. However, if any part/section (and thereof) of this document is not applicable for a project or if one is tailoring any part/section of this PMP template; please provide the rational/justification as to why it was tailored or why any given part/section of this document was not applicable for this project.

This introductory page describes the purpose of this document (i.e., PMP template) and should be deleted when creating a project PMP.

EXECUTIVE SUMMARY

Briefly define the intended audience and describe the scope of the plan. The scope of a PMP is the following:

- Identify stakeholders, objectives, assumptions and constraints
- Tailor the SDLC framework
- Define the structure of the project organization
- Define the approach to integrate acquisition, engineering, quality assurance, configuration management, security, verification & validation
- Create the project integrated master schedule
- Define the staffing profile
- Define the management/technical infrastructure environments
- Estimate the life cycle costs
- Plan the System Verification & Validation
- Identify Project Classification Schema (Size, Risk, and Class)

1 OVERVIEW

1.1 Purpose

Describe the purpose, scope and objectives of the project. Explain how they fit within a broader vision of any overall program or product life cycle. Describe what is out of scope as well. Describe the business or system needs being satisfied by the project. Provide a reference to any requirements descriptions that drive this project, and expected outcomes.

1.2 Background

Describes why the project is important to the organization, its mission, and the capabilities the project will provide to the organization. Include any background or history that is important to understanding the project.

1.3 Points of Contact

Identify the key points of contact for the project management plan including the major stakeholders.

Role	Stakeholder Name	Phone Number	Email
Division Director			
Business-line Customer/ Sponsor			
Government PM			
Contractor PM			
<others>			

TABLE 1-1: POINTS OF CONTACT

1.4 Project References

Provide a list of documents and other sources of information referenced in the plan. Include for each the title, report number, date, author, and publishing organization. Include a reference for the authorizing document for this project, the Statement of Work or Marketing Requirements or Charter or whatever that might be for the organization.

2 PROJECT ORGANIZATION

Describe the organization for the project, using the sections that follow. Include an organization chart that defines the Government key positions as well as the contractor positions.

2.1 Governance

Define the governance structure and any proposed changes for this project. This will include committees (user groups, Integrated Product Teams (IPT), etc) and authorities that will be involved in the review and approval of work products for the project.

Committee	POC	Role
IPT		
CCB		▪ Approving/disapproving all SCRs/requirements for a system/project[1] ▪ Approving the scope, SCRs/requirements, budget, and schedule for all planned projects ▪ Enforcing the various milestones related to the project date (e.g., Scope definition, code freezes, go/no-go decisions, etc.) ▪ Establishing "One-Voice" communication and direction for the system/project with all key stakeholders
PMO		
<others>		

TABLE 2-1: GOVERNANCE

2.2 Staffing Plan

Specify the numbers and types of personnel required for the Project. Required skill levels, start times, duration of need, and methods for obtaining, training, retaining, rotation, and the phasing out of personnel should be specified. The roles assigned to team members should also be maintained as a part of the staffing plan.

2.3 Training Plan

The Training Plan is developed and describes the training that is needed for the project team. In general, training may be required when a project team is using a new tool/technology or when a project team is unable to find resources with the required skills. For the training plan, specify the set of skills needed, when those skills are needed, the skills for which training is required through formal ways (i.e. training programs etc.) and the skills that will be obtained through informal ways (i.e. on-the-job training, informal mentoring etc.). The training could be Role based or Project based. The mechanism for assessing the training effectiveness should be mentioned in the plan as well as tracking the training details (who, when, mechanism, etc.).

2.4 Project Team Roles and Responsibilities

The following section defines the specific roles and responsibilities of both the government and Contractor personnel supporting each project. It is recognized that for many projects, the same person may fulfill multiple roles. For example, the FAS OCIO Division Director may also be the FAS OCIO

[1] It is expected that a specific criteria are defined for SCRs/requirements requiring CCB approval. For SCRs/requirements not meeting these thresholds, the CCB Chairperson (or other person designated) acts in this role and approves the SCR/requirement (through a documented process). A listing of these SCRs/requirements can then be provided to the CCB members as appropriate.

Project Manager. However, these roles still exist. Additionally, it doesn't delineate every role that may exist on the Contractor Project Team. It defines the key roles that typically exist.
The following descriptions are general in nature and each project should tailor these descriptions as appropriate.

Role	Responsibilities	Name
Division Director	▪ Ensure that the project is following all applicable General Services Administration (GSA)/FAS/Federal rules and regulations and taking corrective action as necessary ▪ Ensure that the project is meeting all applicable FAS Business Goals and Objectives ▪ Establish the communication point between FAS OCIO, FAS Business Lines, the Contractor, and other Stakeholders ▪ Support the FAS OCIO Project Manager in the day-to-day operation of the Project	<name>
Government Project Manager	▪ Develop a fully-integrated project schedule according to the SDLC Project Schedule Template and establishing buy-in with all key stakeholders involved with the project ▪ Monitor the progress of the schedule; take corrective action as appropriate; and communicate/coordinate status with the other stakeholders as necessary ▪ Work closely with the Contractor and the other FAS OCIO stakeholders to ensure that the objectives of the project are being met and take corrective action as appropriate ▪ Ensure that all appropriate FAS OCIO processes and policies (e.g., Configuration Control Board (CCB), Configuration Management (CM), QA, Requirements Management, Security, Budget, Earned Value Management (EVM), etc.) are being followed by the project team ▪ Ensure that decisions made by the CCB (e.g., scope, project dates, “freeze” dates, SCRs, etc.) are being supported by the various stakeholders and report any problems to the FAS OCIO Division Director ▪ Work closely with the Contractor to ensure that all deliverables are meeting the objectives of the contract while meeting the quality standards of FAS OCIO	
Contractor Project Manager	▪ Work closely with the FAS OCIO Project Manager to ensure that the project is successfully meeting its objectives while fulfilling the terms of the contract/SOW ▪ Work with the FAS OCIO Project Manager to develop a fully-integrated project schedule according to the SDLC Project Schedule Template; monitor the progress of this schedule; take corrective action as appropriate; and communicate status ▪ Develop deliverables as required by the SOW and ensure that these deliverables meet the Contractor and FAS OCIO quality standards; and are signed-off	

Role	Responsibilities	Name
	by the appropriate stakeholders ▪ Ensure that all appropriate Contractor and FAS OCIO processes and policies (e.g., CCB, CM, QA, Requirements Management, Security, Budget, EVM, etc.) are being followed by the Contractor Project Team; and communicate known problems to the FAS OCIO Project Manager	
Quality Assurance Team Lead	▪ Help the project to ensure that the FAS OCIO quality standards are being met and appropriate processes are being followed ▪ Provide guidance on Lifecycle tailoring to ensure that the appropriate activities, reviews, and deliverables are included given the scope, schedule, constraints, and risks of the project ▪ Verify that the approved processes are being followed for each project ▪ Verify that required deliverables are being developed for each project ▪ Support the CCB by providing required input to the CCB as requested, attend the various CCB meetings, and support any decisions made by the CCB	<name>
Technical Team Leader	▪ Work closely with the project team to ensure that the technical objectives and standards of the project are being met while following the appropriate FAS SDLC and supporting processes ▪ Work with the Project Manager to develop a fully integrated project schedule, monitor the progress of this schedule, and take corrective action as necessary. ▪ Provide technical direction to the technical staff	<name>
Configuration Management Lead	▪ Implement the CM Process in accordance with the project's CM Plan ▪ Ensure that baselines are established at the appropriate times during the project's lifecycle and CI is under CM control ▪ Support the CCB by providing required input to the CCB as requested, attend the various CCB meetings, and support any decisions made by the CCB	<name>
Test Lead	▪ Manage the activities of the test team to include create test plans; perform the various tests and report results; and produce required documentation ▪ Work with the technical team throughout the entire lifecycle to the product meets the objectives and requirements of the project	<name>
Contractor Project Team	▪ Support the Project Manager in the development of all project deliverables ▪ Follow the SDLC and all approved processes (e.g., CM, QA, Test, Requirements Management, Risk Management, various reviews and walkthroughs, SCRs, etc.) ▪ Follow the approved project schedule and inform the Project Manager of any discrepancies or anticipated	

Role	Responsibilities	Name
	problems in meeting the schedule ▪ Provide the Project Manager with frequent communication on the status of their assigned work ▪ Ensure that their work products meet the Contractor's and FAS OCIO quality standards and accurately reflect the current requirements and design of the system	
Security	▪ Approve that the system meets all applicable GSA/Federal Security Policies ▪ Provide input to the planning, requirements, and design of the project ▪ Approve all security related deliverables including the Requirements Documents, Security Risk Assessment, System Security Plan, CM Plan, and Security Scanning Report ▪ Provide representation on the CCB, providing required information to the CCB as requested, and supporting any decisions made by the CCB	<name>
Requirements Lead	▪ Manages requirements gathering and creation of the requirements documents ▪ Works with the project team to ensure these requirements are appropriately addressed throughout the entire lifecycle and updated as required ▪ Acts as liaison between the business lines and the technical teams.	<name>
Others	<definition>	<name>

TABLE 2-2: PROJECT ROLES AND RESPONSIBILITIES

2.5 Other FAS Stakeholders Roles and Responsibilities

This section defines the major stakeholders for a project, their responsibility for the project, and the frequency of their involvement.

2.5.1 Business Lines

The Business Lines are involved at defined stages and milestones throughout the lifecycle and are critical in the success of the project. These stages may include requirements reviews, CDR, User Acceptance Test, and closing SCRs. The business lines specific responsibilities include:

- Providing input to the scope of the project including the requirements and design
- Defining the requirements/SCRs and providing them to the development team
- Providing representation on the CCB, providing required information to the CCB as requested, and supporting any decisions made by the CCB

2.5.2 Infrastructure

The Infrastructure Team (i.e., Applied Engineering) is involved throughout the entire lifecycle with frequent coordination points and status updates. The Infrastructure Team's specific responsibilities include:

- Providing all hosting functions including development, test, and operational environments
- Working with the project team to ensure that their hosting requirements are adequately addressed given the constraints of the various environments
- Working with the project team to develop appropriate Service Level Agreements (SLAs) and ensure that they are meeting the SLAs
- Providing representation on the CCB, providing required information to the CCB as requested, and supporting any decisions made by the CCB

2.5.3 Interfacing Projects/Systems

The Project Managers of the various projects that the system has an interface with, need to be involved throughout the entire lifecycle with frequent coordination points and status updates. This helps to ensure that the interface is being adequately addressed in terms of requirements, schedule, priorities, design, and other related areas throughout the lifecycle. The Interfacing Projects/Systems specific responsibilities include:

- Working with the project team to ensure that the interface requirements are being met according to both project teams schedule and constraints. This is especially important when one or both of the teams are undergoing a major enhancement to their system or interface
- Supporting the CCB by providing required input to the CCB as requested, attending the various CCB meetings, and supporting any decisions made by the CCB

3 MANAGERIAL PROCESS PLANS

Describe the project management processes for the project. These sections may evolve over the project's lifetime and only a subset of them may stay relevant; use elements accordingly. If there are documented processes that the project team is following, the plan may refer to the documented processes rather than reproducing them.

3.1 Assumptions and Constraints

Describe assumptions on which the project is based and any constraints being imposed in areas. Examples may include schedule, budget, resources, products to be reused, technology to be employed, products to be acquired, and interfaces to other systems/products. Include system dependencies that will affect this project.   Answer Y/N whether the assumption/constraint is being tracked as a separate risk.

Assumptions and Constraints	Impact to Plan	Being Tracked as a Risk (Y/N)

TABLE 3-1: ASSUMPTIONS AND CONSTRAINTS

3.2 Work Plan

Describe the work activities, schedule, resources, and budget details for the project. Much of this content may be in included as part of the project schedule that are maintained as living documents supported by project planning and tracking tools. Include at a minimum, a list of key elements in the project work breakdown structure (WBS) and a description of those activities. If WBS is developed in elements other than "work activities," adapt the descriptions to conform to those elements:

- **Work Activities –** Specify (or refer to a location for) the work activities and their relationships depicted in a WBS. Decompose the structure to a low enough level to facilitate sound estimating, tracking and risk management. Work packages may be built for some or each of the elements of the WBS, detailing the approach, needed resources, duration, work products, acceptance criteria, predecessors and successors. The work activities for this project are as identified in the project schedule. An overview of the project schedule is included in the appendix of this document.
- **Schedule Allocation –** Specify (or refer to a location for) the schedule for the project, showing sequencing and relationships between activities, milestones, and any special constraints.
- **Resource Allocation –** Identify (or refer to a location for) all project team members and their roles. If this information is part of the project schedule, verify that each task is fully resource loaded and in a logical manner (e.g., no resource is more than 100% allocated; for resources that are not 100%, verify that they are working other projects; etc.) If this information is not contained within the project schedule, please use the following table:

Name	Role	Duration	
		Start Date	End date
Name	Tester		
Others			

TABLE 3-2: PROJECT MEMBERS AND ROLES

- **Budget Allocation –** Define the location of the detailed budget information and verify that the budget meets the budget defined by FAS OCIO Planning and Architecture Division.

3.3 Risk Management Plan

Describe or refer to existing processes that will be used to identify, analyze, build mitigation and contingency plans, and manage the risks associated with the project. Describe mechanisms for tracking the specific risks, the mitigation plans, and any contingency plans. Risk factors that should be considered when identifying the specific project risks include contractual risks, organization-related risks, technological risks, risks due to size and complexity of the product, risks in personnel acquisition and retention, risks in achieving customer acceptance of the product, and others specific to the context of the project.

If a program level Risk Management Plan exists for this project, include the reference to the Risk Management Plan and define the location of the risk register for the project. The specific risks for this project, the mitigation actions, and the contingency plans are likely to be documented in another document that is a living record of the current risk information.

3.4 Issue Management

Discuss the resources, methods, and tools to be used for reporting, analyzing, prioritizing, and handling the project issues. Issues may include problems with staffing or managing the project, new risks that are detected, missing information, defects in work products, and other problems. Describe how the issues will be tracked and managed to closure.

If Issue Management is being addressed as part of the Risk Management Program, please state so.

3.5 Control Plan

Describe how the project will be monitored and controlled, using the following areas. For all areas, if there exists another plan that defines this information (e.g., Program Level Plan, separate plan that covers the topic area, etc.), include the reference to the corresponding plan. For any areas that are not applicable to this project, include a justification as to why the corresponding control plan is not needed.

- **Requirements Management –** Describe or refer to existing processes that will be used for measuring, reporting, and controlling changes to the requirements such as: configuration management of the requirements, requirements traceability, impact analysis for proposed changes, and approving changes (such as a Change Control Board).

- **Schedule Control –** Describe or refer to existing processes that will be used for monitoring and controlling the schedule, (e.g. EVM reporting,, milestones, activities, corrective actions upon serious deviation from the plan), frequency of status reporting by team members to the Project Manager (PM) and reporting by PM to the Program Manager and other relevant stakeholders, and what tools and methods will be used.

- **Budget Control –** Describe or refer to existing processes that will be used for monitoring and controlling budget performance controlled. These processes will address how the actual cost will be tracked to the budgeted cost, how corrective actions will be implemented, at what intervals cost reporting will be done for both the project team and management, and what tools and techniques will be used. Include all costs of the project, including contract labor and support functions.

- **Reporting and Communication Plan –** Describe or refer to existing processes/mechanisms, formats, frequencies and information flows that will be used for communicating status of the project work, progress of the project, and other information as needed by the project.

- **Quality Control –** Describe or refer to existing processes/mechanisms that will be used for measuring and controlling the quality of the work processes and resulting work products. Mechanisms used may include verification and validation of the work products, joint reviews, audits and process assessments.

- **Measurement Plan –** Describe how the project measures will be selected (may be a project team effort, based on key issues faced by the project; may be set by external requirements; may be organization standards). Describe how the measures will be collected, analyzed, reported, and used. Include any performance measures that will be used to assess the business impact of this project, including the gathering or development of current baseline values. For many of the projects within a large Program, there may be an applicable Quality Assurance Surveillance Plan (QASP) and therefore, one will not be required at the project level.

3.6 Closeout Plan

Describe the plan for closing out this project. Include descriptions of how staff will be reassigned, project materials archived, and how post-project analysis will gather and document lessons learned and analysis of project objectives achieved. Include an examination of the initial cost/benefit analysis to see if objectives have been met; examine any performance measures intended to be impacted by the project. Include knowledge transfer plan.

If this project is to be followed by a next release effort, operations and maintenance, or other transition plan, describe how those efforts will be planned.

4 TECHNICAL PROCESS

Describe the technical life cycle processes for the project. If there are documented processes that the project team is following, the plan may refer to the documented processes rather than reproducing them. The tailoring of any life cycle processes will be described here as well as technical methods, tools, infrastructure, validation & verification, acceptance plan, and concept of operations.

4.1 Project Classification Schema

This project is a project class *{insert project class}* based on the Project Classification Schema.

4.2 Project Specific Tailoring

Capture any project specific tailoring in the following table for review and approval based on the recommended list of SDLC deliverables defined by the project classification schema. Any deviations are to be documented in the following table; otherwise, all deliverables and phases are expected to be part of the project and match with the project schedule. The project can be tailored to adjust:

- The formality of activities, reviews, and artifacts.
- The overall number of artifacts by merging required elements.
- The number of stages by combining them while providing adequate opportunity for oversight activities.
- The level of detail in specific artifacts.

Deliverables	Project Class				Deliverable Created for this Project (Y/N)	Tailoring Justification
	1	2	3	4		
Security Risk Assessment		X	X	X		
Tools-based Requirements Documentation	X	X				
Active Risk Register		X	X	X		
Risk Management Plan				X		
Business Case (OMB Exhibit)			X	X		
Concept of Operations (ConOps)				X		
Project Management Plan (PMP)/PMP-Lite		X	X	X		
Configuration Management Plan (CMP)				X		
Quality Assurance Plan (QAP)				X		
System Security Plan (SSP)		o	X	X		
Functional Requirements Document (FRD)			X	X		
Requirements Traceability Matrix		o	X	X		
Interface Control Document (ICD)		o	o	X		
Privacy Act Notice/Privacy Impact Assessment		X	X	X		
Test Plan (PT)		X	X	X		
System Design Document (SDD)		o	X	X		
Implementation Plan (IMP)				X		
Maintenance Manual (MM)		o	o	X		
Operations Manual (OM)		o	o	X		
(System Administration Manual)		o	o	X		
Training Plan (TP)		o	o	X		
User Manual (UM)		o	o	X		
Test Files/Data/Cases	X	X	X	X		
Test Analysis Report (TAR)	X	X	X	X		
Test Problem Report	X	X	X	X		
*IT Systems Security Certification & Accreditation		X	X	X		
Security Vulnerability Scan	o	o	X	X		
Post-Implementation Review (PIR)				X		
In-Process Review Report (IPR)				X		
User Acceptance Report	X	X	X	X		

Legend:

X=Required

o= update the Overall System Document as necessary

Blank=Optional

NOTE: This list of SDLC deliverables is not the complete list called out by the SDLC. This list represents the current deliverables that are required/recommended given our current landscape of projects across FAS OCIO.

TABLE 4-1: SDLC TAILORING BASED ON PROJECT CLASSIFICATION SCHEMA

4.3 Methods, Tools, and Techniques

Identify the computing system(s), development method(s), programming language(s), team structure(s), standards, policies, procedures, and other notations, tools, techniques, and methods to be used to develop the work products or services for the project. Include the key elements used to specify, design, build, test, integrate, document, deliver, modify, operate or maintain the project deliverables or services.

The following tools are used within this Division and are applicable to all projects unless stated otherwise in the specific project's project plan.

Tool Type	Specific Tool	Location or URL
Requirements Management		
Change Control (SCRs)		
Configuration Control		
Risk Management		
Issue Management		
Test Case Management		
Project Scheduling		
List all Testing Tools		
List all Development Tools		

Table 4-2. Tools

4.4 Infrastructure Plan

Present the plan for establishing and maintaining the project work environment (hardware, software, facilities), as well as any policies, procedures, and standards needed for the project. If this function is being provided by Applied Engineering or outsourced to another organization, please specify.

4.5 Acceptance Plan

Describe (or refer to a separate document that provides) the plan for acceptance of the project deliverables by the customer or acquirer of the product. Include the objective criteria to be used for acceptance. Describe roles and responsibilities for reviewing the plan, generating the acceptance tests, running the tests, and reviewing results. Describe the final approval process for product acceptance.

4.6 Configuration Management (CM) Plan

Detail (or refer to the description of) the processes, methods and tools that will be used for CM. Include these areas, where applicable: configuration identification, change control, auditing of configurations and configuration items, reporting of status, setting up and controlling the software libraries, and release management. Change control processes should support reporting, review, approval, and tracking of change requests for product requirements changes, work product defects, and project process changes.

If a program level CM Plan exists for this project, include the reference to the CM Plan.

4.7 Test Plan (PT)

Describe (or refer to the description of) the processes, techniques, and tools that will be used for verification and validation of the work products and activities. Identify the types of testing that will be done throughout the life cycle, and which roles will be involved in each (such as unit testing, module testing, integration testing, system testing, and acceptance testing). For each type of testing, describe who will plan the tests, review the plans, develop the tests, test the product, and review the test results.

4.8 Quality Assurance (QA) Plan

Describe (or refer to the description of) the processes, techniques, and tools that will be used for assuring that the project meets its commitments to plans, standards, and processes, and that it demonstrates that the products meet the agreed-to requirements. Include in this description any reviews and audits in support of QA, as well as what roles are performing those. Identify the processes and standards that will be followed by the project, both internal to the organization and any industry or regulatory standards that apply.

If a program level QA Plan exists for this project, include the reference to the QA Plan.

4.9 Project Reviews

This project will report activities, progress, and issues during the Program's established cycle and at the end of the project after project close.
Table 4- presents the stage reviews planned for this project.

Stage	***Review Activity***	***Audience***
Planning	*Review and approve:* ▪ *Basis of Estimate (BOE)* ▪ *Schedule* ▪ *Project Plan* ▪ *List of Requirements/SCRs*	
Requirements Analysis	*Review and approve:* ▪ *Plan* ▪ *Updated: Project Plan as appropriate* ▪ *Updated Requirements/SCR list*	
Test Readiness	*Review and validate as ready:* ▪ *System Software* ▪ *Unit test results* ▪ *Revisions of:* – *Systems Documentation*	
Deployment Readiness	▪ *Test files and/or data* ▪ *Test Analysis Report* ▪ *Problem Report*	

Table 4-3. Project Reviews

APPENDIX A. ABBREVIATIONS, ACRONYMS, AND DEFINITIONS

The following abbreviations, acronyms, and definitions are used in this document.

Abbreviation	Definition
CCB	Configuration Control Board
CIO	Chief Information Officer
CM	Configuration Management
EVM	Earned Value Management
FAS	Federal Acquisition Service
GSA	General Services Administration
IPT	Integrated Project Team
OCIO	Office of the Chief Information Officer
QA	Quality Assurance
PM	Project Manager
PMP	Project Management Plan
SCR	System Change Request
SDLC	Systems Development Lifecycle

APPENDIX B. PROJECT SCHEDULE

Include the project schedules, and other additional documents that are pertain to this Project Plan (At the minimal; please provide the document title, version, and location etc)

[Project Name]Project Management Plan Template - Lite *(PMP)*

(Version 1.0)

Federal Acquisition Service (FAS)

February 1st, 2012

TABLE OF CONTENTS

TABLE OF FIGURES

REVISION HISTORY

Version Number	Description	Date
Version 1.0	Initial Version	February 1st, 2012

{PROJECT NAME} PROJECT MANAGEMENT PLAN - LITE

1. OVERVIEW

1.1 Purpose

The purpose of this Federal Acquisition Service (FAS) Project Management Plan (PMP) template is to define the PMP for various projects within FAS OCIO that do not require the full-scale PMP defined by the SDLC. For the text in the various sections that are in italics, the text may be considered boilerplate information but it should be tailored for each project as it may not apply in totality as written. The Project Management Plan-Lite is meant to cover the following:

- *Project Class 2 and Class 3*
- *O&M releases*

1.2 Reference Documents

In order for a project to create a PMP-Lite, there must exist a Program Level PMP which addresses the managerial and technical processes applicable to these projects. Include the reference to Program Level PMP in this section.

Also include the detailed schedule as a reference but be sure to include the schedule as part of the PMP-Lite package.

1.3 Scope

Describe the overall purpose of this project including description of the high level functionality and a list of all the SCRs/RTM and corresponding description contained within this project. If a separate document defines the SCRs/Requirements, please include the reference to the document.

SCR or Requirement Number	Description

Table 1-1. SCRs/Requirements

1.4 Assumptions and Constraints

Describe assumptions on which the project is based and any constraints being imposed in areas such as schedule, budget, resources, products to be reused, technology to be employed, products to be acquired, and interfaces to other products. Include system dependencies that will affect this release. It may be useful to portray these in a table.

Assumptions and Constraints	Impact to Plan if not True

Table 1-2. Assumptions and Constraints.

2. STAKEHOLDERS

2.1 Project Team

Table 2-1 identifies all project members and their roles:

Role	Point of Contact	Email
Project Team		
Division Director		
Government PM		
Contractor PM		
Test Lead		
Configuration Management Lead		
Risk Manager		
Quality Assurance Lead		
Requirements Manager		
ISSO		
All other project roles		

Table 2-1. Project Members and Roles

2.2 Other Key Stakeholders

Table 2-2 identifies all other key stakeholders and their roles:

Role	Point of Contact	Email
FAS Business Line		
Requirements		
User Group		
Acceptance Testers		
FAS OCIO		
Applied Engineering Point of Contact		
Security Point of Contract		
CCB Chair		
Other key stakeholders		

Table 2-2. Other Key Stakeholders and Roles

2.3 Governance Boards and Authorities

Table 2-3 defines the governance structure and any proposed changes for this project. This will include committees (user groups, Integrated Product Teams (IPT), CCBs, etc) and authorities that will be involved in the review and approval of work products for the projects.

Governance Boards/Authorities	Review/Approval Process
CCB	

Table *2-3*. Governance Boards and Authorities

3. TOOLS

Table 3-1 defines the following tools that are being used within this project.

Tool Type	Specific Tool	Location or URL
Requirements Management		
Change Control (SCRs)		
Configuration Control		
Risk Management		
Issue Management		
Test Case Management		
Project Scheduling		
List all Testing Tools		
List all Development Tools		

Table 3-1. Tools

4. PROJECT CLASSIFICATION, PROJECT DELIVERABLES, AND TAILORING JUSTIFICATION

Define the project class for this project based on the project classification schema.

For each deliverable identified by the following table (i.e., project classification schema), indicate whether it is required for this project and a justification for any tailoring.

	Project Class				Deliverable Created for this Project (Y/N)	
Deliverables	1	2	3	4		Tailoring Justification
Security Risk Assessment		X	X	X		
Tools-based Requirements Documentation	X	X				
Active Risk Register		X	X	X		
Risk Management Plan				X		
Business Case (OMB Exhibit)			X	X		
Concept of Operations (ConOps)				X		
Project Management Plan (PMP)/PMP-Lite		X	X	X		
Configuration Management Plan (CMP)				X		
Quality Assurance Plan (QAP)				X		
System Security Plan (SSP)		o	X	X		
Functional Requirements Document (FRD)			X	X		
Requirements Traceability Matrix		o	X	X		
Interface Control Document (ICD)		o	o	X		
Privacy Act Notice/Privacy Impact Assessment		X	X	X		
Test Plan (PT)		X	X	X		
System Design Document (SDD)		o	X	X		
Implementation Plan (IMP)				X		
Maintenance Manual (MM)		o	o	X		
Operations Manual (OM)		o	o	X		
(System Administration Manual)		o	o	X		
Training Plan (TP)		o	o	X		
User Manual (UM)		o	o	X		
Test Files/Data/Cases	X	X	X	X		
Test Analysis Report (TAR)	X	X	X	X		
Test Problem Report	X	X	X	X		
*IT Systems Security Certification & Accreditation		X	X	X		
Security Vulnerability Scan	o	o	X	X		
Post-Implementation Review (PIR)				X		
In-Process Review Report (IPR)				X		
User Acceptance Report	X	X	X	X		

Legend:

X=Required

o= update the Overall System Document as necessary

Blank=Optional

NOTE: This list of SDLC deliverables is not the complete list called out by the SDLC. This list represents the current deliverables that are required/recommended given our current landscape of projects across FAS OCIO.

Table 4-1. Project Deliverables

5. ACRONYMS

Acronym	Definition
CIO	Chief Information Officer
CM	Configuration Management
FAS	Federal Acquisition Service
EVM	Earned Value Management
GSA	General Services Administration
OCIO	Office of the Chief Information Officer
PM	Project Manager
PMP	Project Management Plan
QA	Quality Assurance
SDLC	Software/System Development Life Cycle
SOW	Statement of Work

User Acceptance Test Report

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

mm/dd/yyyy

Prepared by:

<Company/Division Name>
<Street Address>
<City, State, Zip Code>

Document History

Version	Description	Date
1.0	Initial Release	MM/DD/YYYY

Table of Contents

1 INTRODUCTION

1.1 Purpose

This User Acceptance Test (UAT) report provides the Office of the CIO (OCIO) of the Federal Acquisition Service (FAS) with the result(s) of the User Acceptance Testing of <specified system functionalities> of the <Program/Project Name> project for the release. (If pilot, specify pilot release.)

Describe the purpose of the UAT.

1.2 Scope

Describe the scope of the UAT Plan identifying the various test cases ran as defined by Table 1-1.

Test Case #	Description
TC #1	<Description>
TC #2	<Description>
…	

Table 1-1. User Test Cases for <Release Name>

1.3 Objective

The overall objective of this document is to provide guidance that will serve as the basis for the stakeholders to make a confident "GO / NO-GO" decision on application readiness, with full understanding of the risks and mitigation plans.

1.4 Background

Table 1-2 defines the different testing rounds, dates conducted, and the participants.

When	Who	Participants
Date 1	Audience	Names of Participants
Date 2	Audience	Names of Participants
Others	Audience	Names of Participants

Table 1-2. UAT Schedule

1.5 References

Please specify the documents and guidance materials used during UAT and if under configuration management (CM) list configuration item used (eg Serena Business Manager(SBM)) and the location (provide URL).

For Example:

The following documents and guidance material are under configuration control in <Configuration Management product used, eg Serena Business Manager> and were referenced and/or used during UAT:

- *<Project Name>Test plan*
- *UAT Test Cases*

Location in SBM for UAT test cases:

http://SBM.fas.gsa.gov/project/test/UAT - May 2012

2 UAT RESULTS

The purpose of this UAT Report is to outline the results of testing. All defects are noted and accounted for. Based on these results, recommendations are made whether to continue to the next phase of <Program/Project Title>.

2.1 Acceptance Criteria

Table 2-1 describes the high level acceptance criteria for the UAT. Examples include: all high-priority defects are closed; All medium priority defects are closed or on an exception basis; and no test case has more than two defects associated with the test case.

If the acceptance test criteria is included in the UAT Test Plan, replace the following table with a reference to the UAT Test Plan and specific section.

UAT AcceptanceCriteria	UAT Description

Table 2-1. UAT Acceptance Criteria

2.2 Summary of UAT Results

Table 2-2 provides a summary of the UAT results.

UAT Total Test Cases	UAT Test Cases Passed	UAT Test Cases Failed

Table 2-2. Summary of Test Results

2.3 Detailed Test Results

Table 2-3 provides UAT test case execution results.

Test Case (TC) ID	Date Tested	Tester	Pass/ Fail	Severity of Defect	Summary of Defect	Closed Prior to Production Release (Y/N)	Comments
TC 1	Date 1	Name					
TC 2	…	…					
…							

Table 2-3. UAT Test Case Results

2.4 UAT Recommendations/Action Items

Table 2-4 provides a summary of any outstanding UAT Recommendations/Action Items.

Action Item#	Description	Point of Contact	Date Due

Table 2-4. Summary of Test Results

APPENDIX A. ABBREVIATIONS, ACRONYMS, AND DEFINITIONS

The following abbreviations, acronyms, and definitions are used in this document.

Abbreviation	Definition
CIO	Chief Information Officer
CM	Configuration Management
FAS	Federal Acquisition Service
GSA	General Services Administration
OCIO	Office of the Chief Information Officer
SBM	Serena Business Manager
TC	Test Case
UAT	User Acceptance Test

APPENDIX B. DEFECT REPORT

Attach the Defect Report. This report should provide a listing of defects including at a minimum defect id, description of defect, priority, and due date. Identify location of the report(provide URL). Each defect should map back to the test cases.

A project is a unique venture with a beginning and an end, undertaken by people to meet established goals within defined constraints of time, resources, and quality. A project is defined regardless of its budget source. In other words, it doesn't matter whether a project funds are defined as DME or O&M - it's still a project.

In our organization a project typically performs one of these functions:

- Develop a new system or service
- Make significant improvements to a system or service
- Improve internal processes or introduce new ones
- Build or significantly enhance infrastructure
- Research new technology for a specific purpose
- Scope and plan extremely large efforts
- Application of major patches and upgrades to software

Some examples of work that are not projects:

- Daily Production Support Activities
    - System administration
    - System operations
    - Break/fix activities
    - Customer Support
- Other operational activities that follow a defined process
- Very small system change requests

When a unit of work is less than 500 hours, we generally do not create a formal project. However, we should not be break work into small pieces to avoid making it into a project. When unsure about whether an effort should be a project or not, contact the PMO at xxx-xxxx.

Project Classification—Sizing Matrix

Project Class	Work Effort * (Hours)
1	< 500
2	500 - 2,000
3	2,001 - 5,000
4	5001 - >20,000

Project Classification—Risk Matrix

Risk Factor	Low 0	Medium 1	High 2	Very High 3	Score
Team Size(# of bodies)	<5	5 – 9	10 – 14	>15	
# Applications involved	1 – 2	3	4	>4 or ones involving interfaces to an external system to FAS	
Technology / Technique / Process	Expert	Familiar	New to FAS OCIO	New technology	
Requirements Understanding	The solution is well defined and sign-off has been established from the major stakeholders	The solution is known but some undefined areas exist and sign-off may not have been established	There is more than one approach to achieving the project goal	The solution is not known or only vaguely defined	
Political Profile / Impact	One business Line	Two Business Lines	External Agencies	Enterprise-wide	
				TOTAL	**0**
				RISK MODIFICATION FACTOR	**0**

Scoring Instructions

0 – 10 No change to

11 – 13 Increase Class 1 level

14 – 15 Increase Class 2 levels

Project Class

Project Class from Sizing Chart	
Risk Modification Factor	0
Project Class	**0**

1 Select the project class based on the work effort	2 Use the risk factors above to determine the risk score for each factor. Record the score in the right column. Compare the risk score to the levels to determine the risk modification factor (0, 1, or 2)	3 Use the Project Class on the subsequent sheets in order to determine the project's SDLC deliverables and project approval/EVM Requirements.

*** - work effort is defined as the total staff hours being charged to a project - regardless of the role (e.g., PM, test, development, etc.)**

0

Deliverables	Project Class				Deliverable Created for this Project (Y/N)	Tailoring Justification
	1	2	3	4		
Security Risk Assessment		X	X	X		
Tools-based Requirements Documentation	X	X				
Active Risk Register		X	X	X		
Risk Management Plan				X		
Business Case (OMB Exhibit)			X	X		
Concept of Operations (ConOps)				X		
Project Management Plan (PMP)/PMP-Lite		X	X	X		
Configuration Management Plan (CMP)				X		
Quality Assurance Plan (QAP)				X		
System Security Plan (SSP)		o	X	X		
Functional Requirements Document (FRD)			X	X		
Requirements Traceability Matrix		o	X	X		
Interface Control Document (ICD)		o	o	X		
Privacy Act Notice/Privacy Impact Assessment		X	X	X		
Test Plan (PT)		X	X	X		
System Design Document (SDD)		o	X	X		
Implementation Plan (IMP)				X		
Maintenance Manual (MM)		o	o	X		
Operations Manual (OM)		o	o	X		
(System Administration Manual)		o	o	X		
Training Plan (TP)		o	o	X		
User Manual (UM)		o	o	X		
Test Files/Data/Cases	X	X	X	X		
Test Analysis Report (TAR)	X	X	X	X		
Test Problem Report	X	X	X	X		
*IT Systems Security Certification & Accreditation		X	X	X		
Security Vulnerability Scan	o	o	X	X		
Post-Implementation Review (PIR)				X		
In-Process Review Report (IPR)				X		
User Acceptance Report	X	X	X	X		

Legend:

X=Required

o= update the Overall System Document as necessary

Blank=Optional

NOTE: This list of SDLC deliverables is not the complete list called out by the SDLC. This list represents the current deliverables that are required/recommended given our current landscape of projects across FAS OCIO.

Activities	Project Class				Notes
	1*	2*	3	4	
Project Initiation Package			X	X	Per the Project Initiation IPT
Project Schedule	X*	X*	X	X	For class 1, minimal schedule requirements - no QA buy-off required; Class 2 - Recommend tailoring of O&M schedule template; Class 3 & 4 - SDLC compliant, QA & Stakeholder sign-off per EVM requirements;
BOE	X*	X*	X	X	
Release/Delivery Plan	X*	X*	X	X	For Class 1&2, this will be the planned delivery date for the requirements/SCRs.
Stakeholder Buy Off	X*	X*	X	X	For each class of projects, the list of stakeholders will be expanded. For Class 1&2, it will include the business line representative and the originator of the SCR.
PMP			X	X	
RTM			X	X	
Monthly Budget/Schedule Performance Reports		SPI, CPI			
EVM Project Approval Form			X	X	
EVMReporting Indices			SPI, CPI, EV, PV, AC, BAC, EAC	SPI, CPI, EV, PV, AC, BAC, EAC CV, SV, ETC	
Monthly EVM Review			Yellow and Red Indices	X	
Monthly EVM Reports			X	X	

* - Scaled back versions

Activities	Project Class				Notes
	N/A	2*	3	4	
Project Initiation Package			X	X	Per the Project Initiation IPT.
Project Schedule		X	X	X	Schedule of planned sprints, duration of each sprint, and LOE/velocity per sprint
~~BOE~~					
~~Release/Delivery Plan~~					
Stakeholder Buy Off					
PMP		X	X	X	Submit initial PMP with EVM Package. It is anticipated that an Agile PMP template will be created.
RTM			X	X	Submit initial roadmap with EVM package. This roadmap is then updated at the beginning of each sprint.
~~Monthly Budget/Schedule Performance Reports~~					
EVM Project Approval Form			X	X	
EVM Reporting Indices			SPI, CPI, EV, PV, AC, BAC, EAC	SPI, CPI, EV, PV, AC, BAC, EAC, CV, SV, ETC	Progress reported against sprints. See "AgileEVM Metrics" for definitions of EVM calculations.
Monthly EVM Review			Yellow and Red Indices	X	
Monthly EVM Reports			X	X	

* - Scaled back versions

Deliverables	**Definitions of Deliverables for an Agile Implementation**
Draft Business Case (DBC)	Same
Security Risk Assessment	Same
Division Level PMP	N/A - At the current time, there will not be Division Level PMPs that address all the Agile projects for that Division.
Tools-based Requirements Documentation	For each sprint, provide user stories and acceptance criteria for that sprint. The tools-based documentation should track each user story to what sprint it was developed along with the other required traceability elements (e.g., verification method, test cases, etc.)
Active Risk Register	Same
Risk Management Plan	Same
Business Case (OMB Exhibit)	Same
Concept of Operations (ConOps)	Same
Project Management Plan (PMP)	Explain the overall objective of the project including scope, roadmap, number of planned sprints, preliminary scope of each sprint, how the team will measure velocity, and how the project team will assess the plan for moving forward. Please note that an Agile PMP template will be created.
Configuration Management Plan (CMP)	Same
Quality Assurance Plan (QAP)	Same
System Security Plan (SSP)	Same
Functional Requirements Document (FRD)	For each sprint, provide user stories and acceptance criteria for that sprint. An RTM should track each user story to what sprint it was developed along with the other required traceability elements (e.g., verification method, test cases, etc.). It is recommended that the "ility" requirements be define early in the project (e.g., scability, useability, performance, maintability, etc.) or specifically planned for in the appropriate number of sprints.
Interface Control Document (ICD)	An ICD will typically be part of either the FRD or the tools-based requirements. However, if a separate ICD is required, it is recommended that it be developed as separate sprints - usually earlier in the lifecycle.
Privacy Act Notice/Privacy Impact Assessment	Same
Test Plan (PT)	Describe how testing is going to be performed as part of each sprint along with the supporting information (e.g., roles/responsibilities, test environment, strategy, etc.). Describe how the various sprints are going to be integrated/tested along with system level/UAT testing. Typically, during the early phases of testing in an Agile project, there will not be a specific test team allocated to this function.

System Design Document (SDD)	In the beginning stages of the project, just minimal information is contained with the SDD with the majority of the document being produced during the later part of the project. Information that should be defined early includes system architecture, high level database design, security controls, and external interfaces.
Implementation Plan (IMP)	Developed during the later stages of the project.
Maintenance Manual (MM)	Developed during the later stages of the project.
Operations Manual (OM)	Developed during the later stages of the project.
(System Administration Manual)	Developed during the later stages of the project.
Training Plan (TP)	Same
User Manual (UM)	Developed during the later stages of the project.
System Software	Same
Test Files/Data/Cases	Same
Test Analysis Report (TAR)	Same
Test Problem Report	Same
*IT Systems Security Certification & Accreditation	Same - work with the Security team to address these requirements. For example, at what sprint (if it's installed), does a C&A become required?
Delivered System	Same
Change Implementation Notice (CIN)	Same
Security Self-Assessment	Same
Post-Implementation Review (PIR)	Same
In-Process Review Report (IPR)	Same
User Acceptance Report	Same

Deliverables	Definitions of Deliverables for a Cloud Implementation
Draft Business Case (DBC)	Same
Security Risk Assessment	Same
Division Level PMP	Same
Tools-based Requirements Documentation	If a cloud solution is being used, it is not adequate to have this information contained within a tool (e.g., SCR system, excel spreadsheet, etc.). Instead, an FRD is required.
Active Risk Register	Same
Risk Management Plan	Same
Business Case (OMB Exhibit)	Same
Concept of Operations (ConOps)	Same
Project Management Plan (PMP)	Same. Be sure to include the vendor providing the cloud solution as part of the roles/responsibilities, POC, etc.
Configuration Management Plan (CMP)	Probably a minimal plan (contained as part of the PMP) unless customer developed software is required). Be sure to address with the vendor how they are handling CM, backup/recovery, etc. This is recommended to be considered while selecting a particular solution.
Quality Assurance Plan (QAP)	Same
System Security Plan (SSP)	Same
Functional Requirements Document (FRD)	The purpose is not to document the detailed requirements of the Cloud solution. Instead, it should define the high level business requirements driving the particular clould solution selected along with the selection criteria. This selection criteria should include security, CM, technical concerns, vendor concerns, etc.).
Interface Control Document (ICD)	An ICD will typically not be required unless the cloud solution will have an interface with a FAS system. Then, an ICD should be developed as a separate document so that the requirements can be managed with the cloud vendor.
Privacy Act Notice/Privacy Impact Assessment	Same
Test Plan (PT)	The purpose of testing a cloud implementation is not to test the detailed requirements of the vendor's system but to assure the product selected meets the business and other requirements as specified by the FRD.
System Design Document (SDD)	The purpose is not to document the design of the Cloud solution. Instead, it should define the particular implementation for GSA's environment. Examples include tailoring, data definitions, high level architecture of the solution, and interfaces with FAS' systems.
Implementation Plan (IMP)	Same but typically scaled back because of the cloud solution.

Maintenance Manual (MM)	Typically not required.
Operations Manual (OM)	Typically not required.
(System Administration Manual)	Typically not required.
Training Plan (TP)	Same
User Manual (UM)	Typically provided by the vendor.
System Software	Typically not required.
Test Files/Data/Cases	Same
Test Analysis Report (TAR)	Same
Test Problem Report	Same
*IT Systems Security Certification & Accreditation	Same - work with the Security team to address these requirements. For example, at what sprint (if it's installed), does a C&A become required?
Delivered System	Typically provided by the vendor.
Change Implementation Notice (CIN)	Typically provided by the vendor.
Security Self-Assessment	Same
Post-Implementation Review (PIR)	Same
In-Process Review Report (IPR)	Same
User Acceptance Report	Same

Requirements Traceability Matrix *(RTM)*

(Version 1.0)

[Program/Project Name]

Federal Acquisition Service (FAS)

mm/dd/yyyy

March 1st, 2012

TABLE OF CONTENTS

REVISION HISTORY

Version Number	Description	Date
Version 0	Initial Release	February 2006
Version 1.0	Broke out as a separate document from the FRD	March 1st, 2012

REQUIREMENTS TRACEABILITY MATRIX

The Requirements Traceability Matrix (RTM) is a method for tracking functional requirements and their implementation through the development process. Each requirement will be recorded in the matrix along with its associated paragraph number. As the project progresses, RTM is updated to reflect each requirement's status. When the product is ready for system testing, the matrix lists each requirement, what product component addresses it and what test verify that it is correctly implemented.

Include columns for each of the following in the RTM:

- Source Requirement Document (FRD, ConOps, etc) and the reference Paragraph number;
- Source Requirement textual Description;
- Requirement’s referenced Paragraph number in FRD;
- Verification Method (identifies how the requirement will be verified)
- Requirement’s Reference number in Test Plan

The format of the RTM at the conclusion of requirements analysis should be similar to the following:

Source Requirement		FRD Paragraph #	Verification Method				Test Plan Reference #
Document/ Paragraph #	Description		A	D	I	T	

Key:

A – Analysis
D – Demonstration
I – Inspection
T – Testing

Exhibit 1-1. Caption-C, TNR 11, Bold, 6 pts after.

As the life cycle progresses, the RTM included in FRD can be used as direct input into the:

- High-Level Design;
- Detailed Design;
- Test Plan; and
- Verification & Validation.